मोबाइल, ऐप और IoT सिक्योरिटी

दुनिया भर में डेटा और डिवाइस की सुरक्षा करना

स्टेट-स्पॉन्सर्ड साइबर हमलों और नुकसान पहुंचाने वालों की ऑनलाइन बढ़ोतरी को देखते हुए, हम मानते हैं कि हमारी प्रोडक्ट और सर्विस ही सहायक हैं क्योंकि उन्हें बेहद सिक्योर बनाया गया है. Google में, हम अपनी विशेषज्ञता को दूसरों से शेयर कर रहे हैं और लोग, संगठन और सरकार की सुरक्षा पर पहले से ज़्यादा ध्यान दे रहे हैं. हम कभी भी सामने आने वाले साइबर जोखिमों से निपटने के लिए समाज को सशक्त बना रहे हैं और हर किसी के लिए एक सुरक्षित माहौल बनाने के लिए साइबर सिक्योरिटी को एडवांस करने पर लगातार काम कर रहे हैं.

हमारे लिए यह ज़रूरी है कि हम दूसरों से आगे रहें और लगातार बढ़ते खतरे से निपटने के लिए अपनी सिक्योरिटी को बेहतर करते रहें, खासतौर से बात जब सभी कनेक्टेड डिवाइस और ऐप को सिक्योर करने की हो. ऐसा इसलिए, ताकि उपभोक्ताओं को ऐसा सुरक्षित माहौल दिया जा सके जहां इस्तेमाल किए जा रहे डिवाइस में उन्हें एजेंसी और विकल्प मिल सकें.

चुनौती

कनेक्टिविटी एक कीमत के साथ आती है

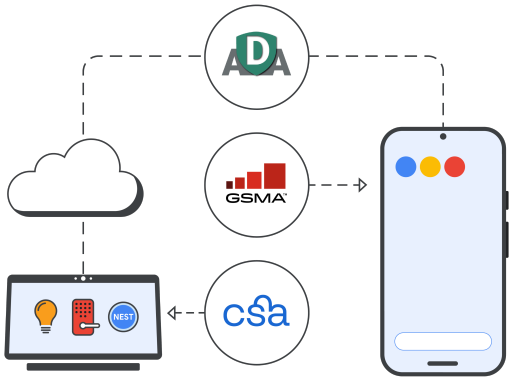
हम अपनी रोज़मर्रा की ज़िंदगी में स्मार्टफ़ोन, ऐप, और IoT डिवाइस का बहुत ज़्यादा इस्तेमाल करते हैं—इस प्रोसेस में ज़्यादा से ज़्यादा समय ऑनलाइन बिताते हैं और ज़्यादा से ज़्यादा ज़रूरी डेटा, जैसे बैंकिंग या स्वास्थ्य से जुड़ी जानकारी शेयर करते हैं. यही वजह है कि संवेदनशील जानकारी पाने के लिए शातिर साइबर अपराधी ऐसे डिवाइस को पहले से ज़्यादा निशाना बना रहे हैं.

ज़्यादा डिवाइस, ज़्यादा डेटा-ज़्यादा खतरे

एक अनुमान के मुताबिक, दुनिया में 17 अरब IoT डिवाइस हैं. इसमें, प्रिंटर से लेकर गैरेज का दरवाज़ा खोलने वाले डिवाइस शामिल हैं, और ये सभी सॉफ़्टवेयर से भरे हुए हैं (कुछ ओपन-सोर्स वाले हैं) जिन्हें आसानी से हैक किया जा सकता है.[1] कुल मिलाकर, असुरक्षित IoT डिवाइस की संख्या 2020 में लगभग दोगुनी हो गई है.[2]

- हालांकि हम IoT डिवाइस के ज़रिए गहराई से जुड़ते जा रहे हैं, लेकिन सिक्योरिटी क्वालिटी का पता लगाने के लिए कोई भी ग्लोबल स्टैंडर्ड नहीं है. इस वजह से, उपभोक्ताओं को बिना जानकारी के ही डिवाइस की सिक्योरिटी से जुड़े फैसले लेने पड़ते हैं.
- उपभोक्ताओं को जिस तरह भोजन या सफ़ाई से जुड़े प्रोडक्ट में डाली गई सामग्रियों को जानने का अधिकार होता है, वैसे ही उनके पास डिजिटल प्रोडक्ट से जुड़ा पारदर्शिता का अधिकार भी होना चाहिए.
- मोबाइल डिवाइस दूसरी तरह के हमलों के लिए एक वेक्टर की तरह काम करते हैं, और डिवाइस की इंटरकनेक्टिविटी बड़े पैमाने पर सिक्योरिटी पारदर्शिता की ज़रूरत को बढ़ावा देती है. इसलिए, नेटवर्क और सिस्टम की सिक्योरिटी की तरह ही कनेक्टेड डिवाइस इकोसिस्टम की सिक्योरिटी भी ज़रूरी है.

इंडस्ट्री संगठनों के साथ हमारी साझेदारी



हमारा समाधान

Google में, हम मोबाइल, ऐप और IoT सिक्योरिटी के ज़रिए अपने कनेक्टेड डिवाइस की सिक्योरिटी और पारदर्शिता को बेहतर बना रहे हैं:

मोबाइल सिक्योरिटी

हमारे ओपन सोर्स ऑपरेटिंग सिस्टम Android में मोबाइल डिवाइस को सुरक्षित रखने के लिए एक लेयर्ड सिक्योरिटी अप्रोच है:

- लेयर्ड सिक्योरिटी
  - वेरिफ़ाइड बूट, रोल-बैक प्रोटेक्शन और फ़ैक्ट्री रीसेट प्रोटेक्शन की वजह से लेटेस्ट, सेफ़ेस्ट Android वर्शन काम करता है.
  - PIN और बायोमेट्रिक ऑथेंटिकेशन शील्ड किसी भी आउटसाइड एक्सेस को रोकती है.
  - अगर डिवाइस चोरी हो जाए या खो जाए, तो 'Find My Device' उसे लोकेट करने या क्लीन करने में मदद करता है.
- पहचान और पासवर्ड प्रोटेक्शन
  - 2-चरणों में पुष्टि, एक Security Key के रूप में फ़ोन, और Password Manager आपके Google अकाउंट में बाहरी एक्सेस को रोकते हैं.
  - सिक्योरिटी चेकअप और वैकल्पिक सबसे मज़बूत सुरक्षा डिवाइस को सुरक्षित और आसानी से चलाने लायक बनाते हैं.
- एंटी-फ़िशिंग प्रोटेक्शन
  - Phone by Google और Messages by Google, स्कैम और फ़िशिंग ोंअटैक का पता लगाने और उन्हें रोकने में मदद करते हैं.
  - Google सुरक्षित ब्राउज़िंग का दुनिया भर में 5 अरब से ज़्यादा डिवाइस की सुरक्षा करता है.

ऐप सिक्योरिटी

आउट-ऑफ़-द-बॉक्स एंटी-मैलवेयर खराब ऐप को बाहर रखने में मदद करता है और ऐप डाउनलोड करते वक्त डेटा सुरक्षा जानकारी यूज़र को पारदर्शिता मुहैया कराती है.

- Google Play Store: मशीन-लर्निंग डिटेक्शन टूल और मानव विश्लेषकों के ज़रिए डाउनलोड के लिए उपलब्ध होने से पहले सभी ऐप की समीक्षा की जाती है. Data Safety सेक्शन बताता है कि ऐप किस तरह का डेटा इकट्ठा करते हैं और उस डेटा का इस्तेमाल कैसे किया जाता है.
- Google Play Protect: हर दिन 125 अरब से ज़्यादा ऐप स्कैन करता है और सिक्योरिटी जोखिमों का पता चलने पर सूचना देता है, ऐप हटा देता है या उसे बंद कर देता है.
- App Defense Alliance (ADA): Google ने App Defense Alliance लॉन्च करने के लिए टॉप मोबाइल थ्रेट डिटेक्शन पार्टनर के साथ काम किया है. यह शेयर्ड इंटेलिजेंस और कॉर्डिनेटेड डिटेक्शन के जरिए Android यूज़र को नुकसान पहुंचा सकने वाले ऐप्लिकेशन (PHA) से बचाने में मदद करता है.

IoT सिक्योरिटी

IoT सिक्योरिटी लेबल किसी डिवाइस पर गोपनीयता और सुरक्षा व्यवहार को साफ़तौर से दिखाते हैं, जैसे कि कौन-सा डेटा इकट्ठा किया जा रहा है.

- हम IoT सिक्योरिटी लेबलिंग स्कीम के लिए पांच मूल सिद्धांतों में विश्वास करते हैं: लाइव लेबल, मूल्यांकन स्कीम, लचीलेपन के साथ सिक्योरिटी बेसलाइन, व्यापक आधार पर पारदर्शिता और अपनाने के लिए इंसेंटिव.
- हम Connectivity Standards Alliance (CSA) और GSM Alliance (GSMA) के साथ काम कर रहे हैं, ताकि मौजूदा और भविष्य में नियमों के पालन से जुड़ी ज़रूरतों के लिए इंडस्ट्री-वाइड सर्टिफ़िकेशन प्रोग्राम को मानकों के मुताबिक बनाया जा सके.

हमारे सिद्धांत

Google में, हम अपने कनेक्टेड डिवाइस की सिक्योरिटी और पारदर्शिता को बेहतर बनाने के लिए 3 मूल सिद्धांत अपनाते हैं:

गहराई से रक्षा: हम सुरक्षा ढांचे में कई परतों का इस्तेमाल करते हैं. ये सभी साथ काम करके एक मज़बूत डिफ़ेंस बनाते हैं और इसकी वजह से डिवाइस आसानी से और असरदार तरीके से काम करता है.

खुलापन और पारदर्शी: पारदर्शिता हमारे सिद्धांत का आधार है. हमारे प्लेटफ़ॉर्म उपयोगकर्ता को जागरूक बनाए रखने और सुरक्षा मज़बूत करने के लिए जानकारी शेयर करने पर हमारा मानना है कि एक ओपन सोर्स इकोसिस्टम क्लोज़ इकोसिस्टम की तुलना में ज़्यादा सिक्योर हो सकता है.

Google और हमारे इकोसिस्टम की सबसे अच्छी बातें: हम अरबों उपयोगकर्ता को सुरक्षित रखने में मदद करने के लिए Google और इंडस्ट्री की विशेषज्ञ टीमों के साथ साझेदारी करते हैं.

ऐप्लिकेशन

IoT सिक्योरिटी लेबल: उपयोगकर्ता के पास कंट्रोल होना

स्थापित IoT सुरक्षा लेबलिंग के बिना, डिवाइस बनाने वाली कंपनियों के लिए नियमों का कोई ग्लोबल स्टैंडर्ड नहीं है.उपयोगकर्ताओं के पास यह विज़िबिलिटी नहीं है जिससे वे जान सकें कि डिवाइस डेटा को प्रोटेक्ट करते हैं या नहीं, जबकि उन्हें इसका अधिकार है. IoT सिक्योरिटी को आगे बढ़ाने और उपभोक्ताओं को नियंत्रण वापस देने के लिए इंडस्ट्री को साथ आने की ज़रूरत है. हम अपनी प्रक्रिया और साझेदारियों के ज़रिए IoT सिक्योरिटी लेबलिंग स्कीम पर काम कर रहे हैं.

- सबसे पहले, हम संभावित खामियों का पता लगाने के लिए आउटसाइड सिक्योरिटी रिसर्च में निवेश करते हैं (Google Nest, Google इनाम प्रोग्राम में हिस्सा लेता है और खामियों का पता लगाने वाले Google से बाहर के सिक्योरिटी रिसर्चर्स को रिवॉर्ड देता है.
- यहां, हम लॉन्च के बाद कम से कम पांच साल के लिए ज़रूरी बग पैच और फ़िक्स जारी करते हैं.
- 2019 और उसके बाद विकसित हुए हमारे सभी डिवाइस वेरिफ़ाइड बूट का इस्तेमाल करते हैं. इससे यह पक्का होता है कि सही सॉफ़्टवेयर काम कर रहा है और एक्सेस प्रोटेक्टेड है. उदाहरण के लिए, हमारे Google Nest डिवाइस की थर्ड-पार्टी, इंडस्ट्री-मान्यता प्राप्त सिक्योरिटी स्टैंडर्ड का इस्तेमाल करके पुष्टि की जाती है, जैसे कि NIST, ETSI, और ISO.

ये मानक और हमारी सिक्योर Software Development Life Cycle (SDLC), उपभोक्ताओं के खराब सुरक्षा तरीकों के संपर्क में आने की संभावना को कम करेंगे और खुलेपन वाले, सुरक्षित इंटरनेट का मज़बूत रास्ता बनाएंगे.

हमारा इंडस्ट्री निवेश और मुकाम

2007 उपयोगकर्ताओं के खतरनाक वेबसाइटों पर जाने पर उन्हें तुरंत सतर्क करने के लिए सेफ़ ब्राउज़िंग को तैयार किया गया और अब यह 5 अरब से ज़्यादा डिवाइस को प्रोटेक्ट करता है.

2010 Google Transparency Report की लॉन्चिंगइसलिए की गई, ताकि ये दिखाया जा सके कि सरकार और कॉर्पोरेट की नीतियां और ऐक्शन कैसे निजता, सुरक्षा, और ऑनलाइन जानकारी के एक्सेस पर असर डालते हैं. 2018 में, हमने Android पर काम करने वाली Transparency Report की शुरुआत की.

2017 Google Play Protect लॉन्च किया गया जो अब सबसे बड़े स्तर पर काम करने वाला ऐंटी-मैलवेयर सॉल्युशन है. यह हर दिन 3 अरब से ज़्यादा डिवाइस में 125 अरब से ज़्यादा ऐप को स्कैन करता है.

2019 सुरक्षा कुंजी को 2020 में Android और फिर iPhone के लिए बिल्ट-इन फ़ीचर के तौर पर पेश किया गया.

2022 Google Play ने एक डेटा सुरक्षा सेक्शन लॉन्च किया, ताकि लोगों को इस बारे में ज़्यादा जानकारी दी जा सके कि ऐप किस तरह उपयोगकर्ता का डेटा इकट्ठा, शेयर और सिक्योर करते हैं और किसी भी ऐप के लिए पहला बैज सिस्टम शुरू किया है जिसने App Defense Alliance के ज़रिए एक अलग सिक्योरिटी समीक्षा पूरी कर ली है.

2023 पासकी: एक ऐसा भविष्य जिसमें बार-बार पासवर्ड डालने की ज़रूरत नहीं होगी, इस पहल को FIDO Alliance और दुनिया भर के टेक दिग्गजों के साथ खुले मानकों को चलाने के एक दशक के बाद एक्सटेंडेड पासकी सपोर्ट के साथ शुरू करने की तैयारी की जा चुकी है.

हमारा नज़रिया

खुलेपन, सिक्योर डिजिटल दुनिया के लिए प्रतिबद्ध

अलग-अलग नेटवर्क पर ज़्यादा डिवाइस के ज़्यादा डेटा, सुरक्षा चिंताओं को और बढ़ाएंगे. हम अपने प्रोडक्ट डेवलपमेंट, पारदर्शिता के पैमाने और इंडस्ट्री साझेदारी के ज़रिए कनेक्टेड डिवाइस सिक्योरिटी के भविष्य को बेहतर करने में मदद कर रहे हैं

हमारी प्रोडक्ट रणनीति का आधार यह पक्का करना है कि हमारे प्रोडक्ट डिफ़ॉल्ट रूप से सिक्योर हैं. सुरक्षित ब्राउज़िंग का, Google Play Protect और बिल्ट-इन सुरक्षा कुंजी हमारे प्रोडक्ट में उच्चतम स्तर की सुरक्षा देकर मोबाइल डिवाइस और ऐप्लिकेशन को प्रोटेक्ट करते हैं.

हम खुलेपन और पारदर्शिता के साथ अपने सिक्योरिटी ऑपरेशन को आसान बनाते हैं. यही वह तरीका है जिससे हम समस्याओं को सुलझाते हैं और कनेक्टेड डिवाइस सिक्योरिटी की जानकारी को शेयर भी करते हैं. हमारा मानना है कि लेयर्ड सिक्योरिटी नज़रिए के साथ एक ओपन सोर्स इकोसिस्टम एक क्लोज इकोसिस्टम की तुलना में ज़्यादा सिक्योर हो सकता है.

CSA, ADA और GSMA के बीच सहयोग करके, हम सभी के लिए सुरक्षित इंटरनेट और भविष्य के लिए साइबर सिक्योरिटी को एडवांस करने की कोशिश करते हैं.

हम कनेक्टेड डिवाइस सिक्योरिटी का स्तर बढ़ाने और हर जगह, हर किसी के लिए एक सुरक्षित ऑनलाइन वातावरण के लिए मानक स्थापित करने के लिए प्रतिबद्ध हैं. कनेक्टेड डिवाइस सिक्योरिटी में Google की प्रगति के बारे में ज़्यादा जानें: g.co/connecteddevicesafety

स्रोत: [1] CNBC Cyber Report, 9 जनवरी, 2023, [2] IoT हमला क्या है? The Ins and Outs of IoT Security, 20 जुलाई, 2021