January 17, 2019

Security Event Timeline

Security Event Timeline

Abstract:

This publication describes a security solution that incorporates security events in a single place and presents them in an easy-to-understand timeline. The intrinsic dynamic essence of the timeline enables the user to see what affects the overall security and offers guidance for the user to take steps to achieve a desired security state. The security solution shows the most-relevant security events at the highest level, but it also allows the user to see all of the security event details, if the user chooses to do so. The user can easily determine the time at which overall security became compromised and can report these changes to the security solution provider or a third-party service or product provider. The security solution displays, in the timeline, important milestone announcements (e.g., Year in Review) — information that can further help the user understand and take steps to increase security.

Keywords: security solution, security product, security event, antivirus software, potentially harmful application (PHA), data breach, security event timeline, privacy setting

Background:

A person's identity, security, and well-being are extensively dependent on data security. To this end, engineers and scientists have created security products. Each security product provider tackles the problem in their own way. In addition, product security providers try to increase security by employing various identifiers (e.g., username, password, personal identification number (PIN), government-issued identification, radar signature, biometric sensors, media address control identification (MAC ID), voice recognition, various sensors, radio-frequency identification (RFID), etc.). Moreover, a user often supplies a multiple-factor (e.g., username and password) authentication to decrease the likelihood of misrepresentation.

Many security products present the user with a security status.[1, 2] For example, an antivirus software may display the status of the last time the user scanned the device for malware, or it may even display the security status with phrases, such as: at risk, fully protected, or perform a scan. As another example, an operating system (OS) may list events, such as: creating, opening, or deleting a file, downloading a third-party software, updating the OS version, OS crash, and other various privacy settings and security events.[1, 2] And, as yet another example, a camera security system with its associated software application may display a message accompanied with a still photograph of an intruder.

Fig. 1 helps illustrate the figurative wallet-content of a typical first-world citizen.

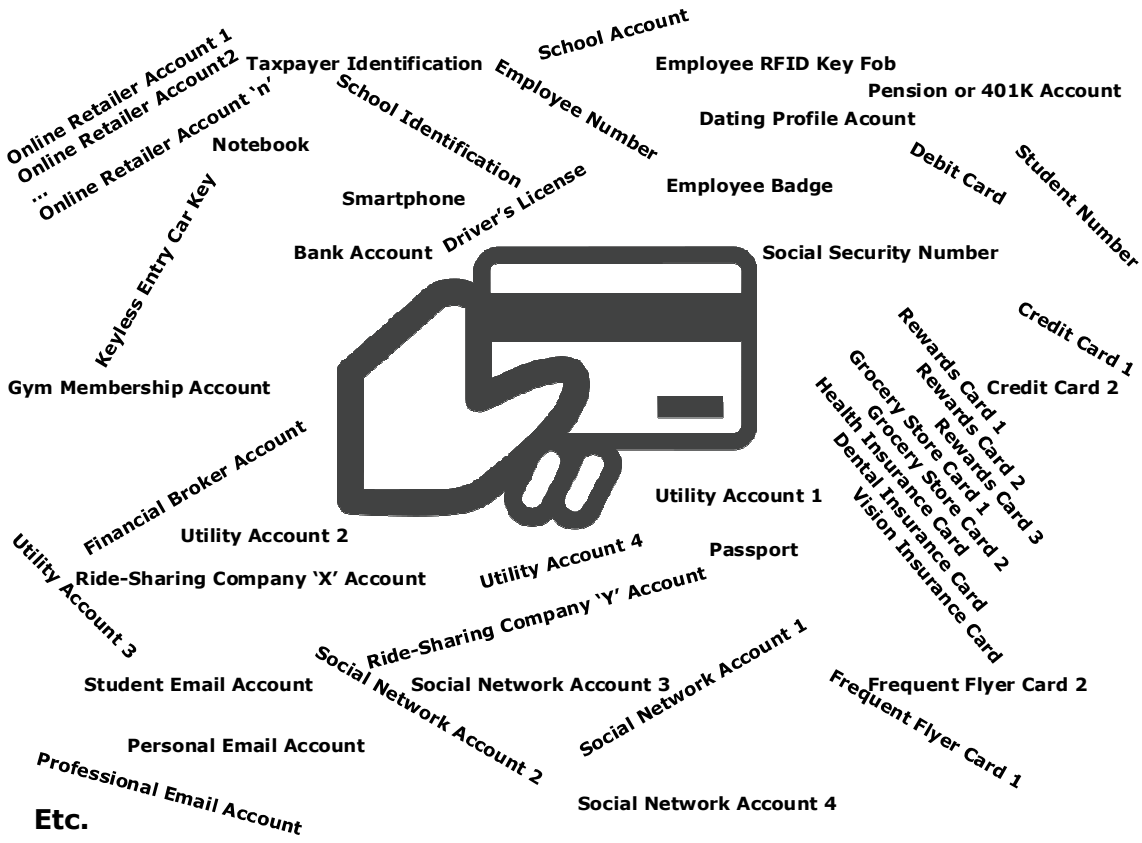

Fig. 1

One might find Fig. 1 absurd, but it is not an exaggeration. The days when a deadbolt lock to the house door was enough to provide peace of mind are gone. In the Information Age, a person routinely manages multiple devices and online accounts. In addition, several of these accounts are interlinked with each-other (e.g., a credit card may be linked to a frequent flyer card). Various operating systems (OS) have helped combine these many profiles, but each product and service provider is often responsible for safeguarding the user's data. In addition, security and privacy settings of these many accounts are scattered across a computer's operating system (OS). Furthermore, the user is often uncertain as to which software application handles which security or privacy setting. Things become even less clear when the user manages device settings,

application software settings, security products settings, internet security and privacy settings, on a single device (e.g., a smartphone).

Even with layers of security, data breaches still occur—often with severe consequences. The modern citizen may benefit from a comprehensive security solution. In addition, the modern citizen needs to have a clear understanding and exert some control over the security solution.

1. *End-User Guides,* https://www.cisco.com/c/en/us/support/security/security-manager/products-user-guide-list.html, accessed on November 27, 2018.

2. *Event Logs*, May 30, 2018, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc722404(v%3dws.11), accessed on November 27, 2018.

Description:

The aim of a security solution is to empower a person to easily understand and take control of her own overall security. This security solution does not merely list privacy events or show the current security status, but it displays privacy settings and security events in a time-sorted sequence, as illustrated in Fig. 2—here on one display.

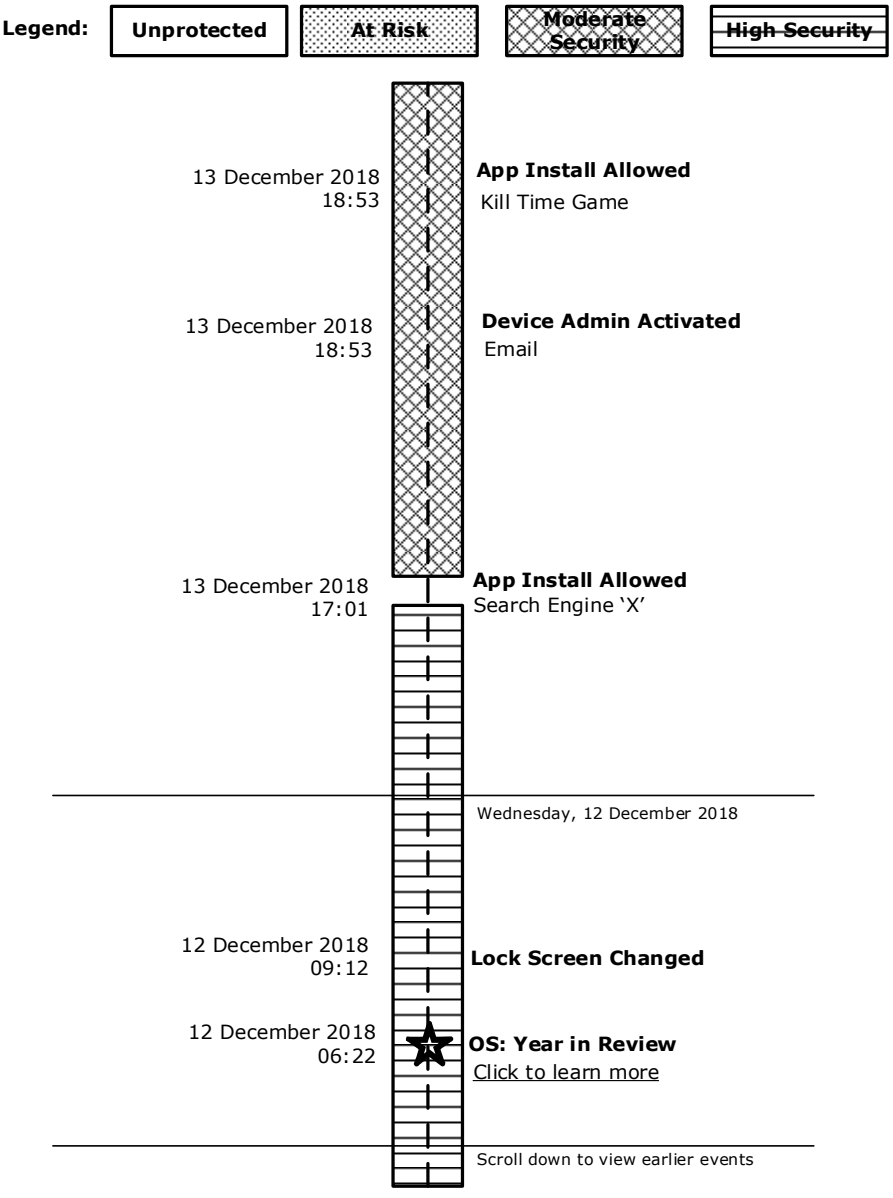

Fig. 2

The time-sorted sequence of privacy settings and security events comprehensively informs the user of the current and past security status. In addition, the security solution informs the user on the events that led to a particular security status. For example, in Fig. 2, when the user downloaded Search Engine 'X', the security solution downgraded the security status from High Security to Moderate Security. Obviously, the security solution makes this determination based on well-established vulnerabilities associated with Search Engine 'X'. The security solution, then, guides the user to take steps to increase the security status (e.g., uninstalling Search Engine 'X').

To communicate the security status, the security solution may use words (e.g., high security, moderate security, low security, at risk, unprotected); may use colors (e.g., green, yellow, orange, red); may use symbols (e.g., a key, a lock, chains, a crowbar, wire cutters); may use patterns, as shown in Fig. 2; and, may use any combination of phrases, colors, symbols, patterns, and so forth. Concurrently, the security solution clearly displays through a timeline how the user reached a certain security status. In addition, the security solution guides and allows the user to take steps to change the security status to a desired state.

The security solution may display the security timeline on various displays (e.g., smartphone screen, television screen, computer monitor, etc.). In addition, the security solution combines all privacy settings and security events regardless of whether they are related to the OS, the security solution itself, or first-party and trusted third-party application software, products, and services. To this end, the security solution supports various application programming interfaces (APIs) to merge the various application software, products, and services.

Fig. 3 helps to further show how this security solution offers a comprehensive security protection at the user's fingertips—all in one easy-to-understand timeline display.

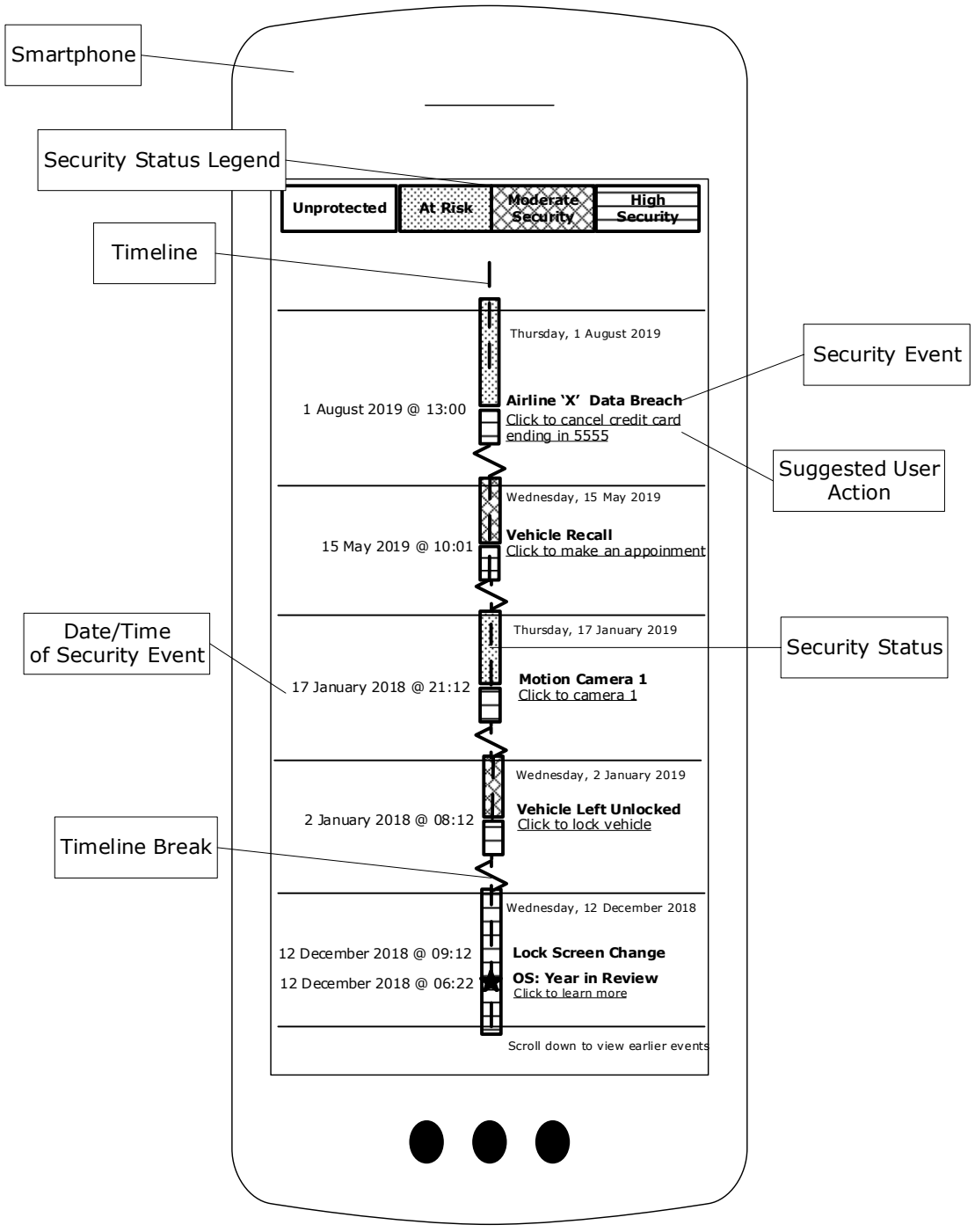

Fig. 3

Consider a user accessing the security solution on a smartphone, as illustrated in Fig. 3. The security solution shows the security status through time. In addition, it shows the events that may affect the overall security of the user. For example:

- The user adds an OS account to a new device. The security solution shows this event in the timeline. In addition, it shows how this event may affect the overall security and may guide the user to take specific steps to reach or keep a desired security state.
- The user left a spare phone turned on (or off). The security solution shows this event and allows the user to keep the spare phone on, or remotely turn it off.
- Someone has tried to login to the user's media-content provider by using the user's email address (or username). The security solution lists this event in the timeline and recommends changing the account password of the media provider.
- The user's favorite airline reports a data breach that resulted in the theft of credit card details. The security solution reports this event in the timeline and provides a link that aids the user to cancel the user's credit card associated with the airline account.
- The user drives to a grocery store and forgets to lock the car. The security solution alerts the user, reports this event in the timeline, and allows the user to use the smartphone to remotely lock the car.
- A car manufacturing company issues a vehicle recall. A person who has downloaded the company's software application receives this announcement in the security solution timeline with a link to make an appointment with the local dealership.

As one can see, one goal of the security solution's merging and showing all security events in a comprehensive timeline is to empower the user to take control of different security events that may affect the user's overall security. Fig. 3 also shows that the security solution places different

weights on different privacy settings and security events. For example, an intruder entering a person's house is more concerning than someone trying to gain access to the user's media subscription.

At the highest level, the user can see application software related events (e.g., installation or uninstallations), security solution events (e.g., potentially harmful applications (PHAs) found), device security events (e.g., login password disabled), and OS account events (e.g., password changes, accessing the account from a new device, etc.). In addition, the security solution allows the user to zoom in to view more granular events (e.g., application software permission requests).

In summary, the described security solution incorporates security events in a single place and presents them in an easy-to-understand timeline. The intrinsic dynamic essence of the timeline enables the user to see what affects the overall security and offers guidance for the user to take steps to achieve a desired security state. The security solution shows the most-relevant security events at the highest level, but it also allows the user to see all of security events details if, the user chooses to do so. The user can easily determine the time at which the overall security became compromised and can report these changes to the security solution provider or a third-party service or product provider. The security solution displays, in the timeline, important milestone announcements (e.g., Year in Review) — information that can further help the user understand and take steps to increase security.