FCC TAC SECURITY & PRIVACY WORK GROUP
CONSUMER EDUCATION RECOMMENDATIONS

INTRODUCTION

This brief paper describes the Security and Privacy Work Group's recommendations pertaining to end user awareness education. These near term recommendations attempt to address the growing gap between the magnitude and complexity of threats and vulnerabilities associated with today's mobile usage environment, and the typical consumer's awareness of security and privacy concerns and attention to countermeasures. In particular, the Work Group feels that there is an urgent need to reach consumers with simple, clear, and consistent messaging, delivered ubiquitously through a high profile public service awareness marketing campaign. Partnering with industry groups is key to fostering a collaborative initiative across industry stakeholders, leveraging and extending existing educational content, and developing support for the ubiquitous dissemination of the content to consumers. This cohesive and systematic educational initiative is a vital component of broader efforts needed to counter the looming crisis around mobile security.

A GROWING REASON FOR CONCERN

The reality is the smartphone has become the information hub, and this role is increasing. The number of smartphone apps is rapidly growing, and the trend is for more connectivity and processing of greater amounts of sensitive information. This is driven by the growing use of online banking, e-wallet, corporate email, local file storage, location tracking services, social networking, direct device-to-device communication, etc. Most of these mobile devices regularly use unsecured public Wi-Fi hotspots to exchange this information, with little regard by most consumers for the significant security implications.

As a result of this information hub trend, the smartphone has become a very rich and highly vulnerable attack target. Several industry studies have shed light on this trend, including a recent statement from Security research firm Kaspersky Labs[1], which stated the volume of new Android malware increased 3X in 2Q 2012, and a similar report from Trend Micro[2] that the number of malicious Android apps doubled from 10,000 to 20,000 in just one month that same quarter. The threats are not just in the form of otherwise benign applications being infected with malware, but also in the form of malicious applications populating application stores. According to RSA[3], mobile applications have emerged as an important cyber crime attack vector for phishing and malware.

Yet, as the threats increase in magnitude and sophistication, there is not a corresponding increase in the application of threat mitigating mechanisms. A September 2012 report by Juniper Research[4] indicated only 5

[1] http://www.kaspersky.com/about/news/press/2012/Android_Under_Attack__Malware_Levels_for_Googles_OS_Rise_Threefold_in_Q2_2012

[2] http://www.trendmicro.co.uk/newsroom/pr/the-true-face-of-the-android-threat

[3] http://www.emc.com/about/news/press/2012/20120725-01.htm

[4] http://juniperresearch.com/viewpressrelease.php?pr=339

percent of smartphones and tablet devices have any form of security software installed. The extraordinarily rapid rate at which phones have transformed into always-on (often Enterprise-connected) general purpose handheld computers, and attractive as mobile platforms for many types of commerce, also makes them very attractive targets for cyber crime. As the mobile devices have settled into two major operating systems (Apple IOS and Google Android) and two second tier OS (RIM and WINDOWS), bad actors have benefited from the "standardization" of platforms to help focus attacks against popular applications and platforms.

Only an end-to-end and collaborative effort, *spanning* the mobile ecosystem (devices/platforms, applications, network services), will make any meaningful progress toward curbing this rapidly growing problem. On the industry side (addressed in companion longer term recommendations), there is a need to increase synergy and coordination across the ecosystem by fostering/extending industry/government partnerships, and by creating new opportunities for information sharing. Equally critical, and urgent to begin now, is the need to holistically and effectively impact consumer awareness of the severity of these threats, and provide clear and consistent guidance on practical safeguards consumers can take to protect their security and privacy.

FACTORING IN CONSUMER REALITIES

Consumers have hungrily adopted generations of ever-more-sophisticated smart mobile device technology for the tremendous productivity, convenience, and entertainment enjoyment delivered. But at the same time, they have demonstrated a relative disregard to the growing security threats and the necessity to bother with security precautions and countermeasures.

Partly this is due to the extraordinarily rapid pace of mobile device advancement, adoption, and usage patterns. It also took many years for PC security tools and adoption to mature - however, the threats in the mobile environment are growing at a much faster pace than they did in the early years of the PC. It will be unfortunate indeed if most users adopt security safeguards only *after* they have suffered a major loss of privacy, time, and money.

It is also true that the rich mobile apps environment encourages sharing of personal information and dynamic interaction between applications, often behind the scenes. Consumers' personal information is guarded at best by opt-in pop-up requests, which many consumers find confusing, annoying, or (say-yes-if-you-want-to-do-*anything*) inflexible. To be effective, controls over information sharing need to be overhauled to be and much more clear, intuitive, and consistent across devices, consumers must be made acutely aware of their importance, and user-friendly guidance must be readily in hand to make effective use of them. Just establishing common definition and labeling of security settings levels, and common robust defaults across device OSs (as suggested in companion best practices recommendations) will go a long way in making the awareness campaign simpler and more effective.

Reaching the diverse population of "typical consumers" requires finding the right balance of contents that will be both effective against the greatest threats, as well as concise enough to be consistently and constantly repeated to build the awareness theme and cement it into public consciousness. Complexity in theme would be the enemy of rapid and complete assimilation of the message into social consciousness. It is important to keep in mind that an important part of the typical consumers that need to be reached are the growing population of smartphone-wielding teens and pre-teens, whose usage and security hygiene routines will be set early-on. As we have seen over the years with public education campaigns for home fire safety (drop and roll) and more recently with "don't text and drive" campaigns, it can be difficult to engage the public (and especially youth) even when the consequences of the behaviors can be life threatening.

The themes and contents to be developed should leverage the best of contemporary marketing practices to ensure they resonate with the target populations. The opportunity to take the “basic” contents and tailor/focus on themes relevant to discrete subsets of the consumer population will also be important. For example as mobile commerce increases it may be that a special theme or message tailored to the known and emerging threats that may attempt to target those users can be developed and delivered to the relevant user populations.

Just as important as forming the right messages, is ensuring that the awareness campaign reaches all consumers. A combination of popular media public service advertising emphasizing awareness, and systematic exposure of actionable guidelines at all device, app store, and wireless service customer touch points is recommended.

In the end, perhaps the biggest challenge in formulating an effective awareness campaign is finding the right balance between the extent of content that experts (and loss experience) may indicate is needed, with the limits of patience and technical sophistication one can reasonably expect from consumers. The recommended guiding principle is: it is much more important to focus on the priority themes, addressing the threats with greatest impact, rather than attempting to be comprehensive.

LEVERAGING THE POWER OF BRANDING

Public service awareness campaign experience dating from Forestry Service success with “Smoky the Bear” and other examples (“McGruff” anti-crime dog, etc.) have demonstrated the benefits to increased public retention and recognition that attend to a well chosen and presented branding campaign. The branding may include a slogan to complement a visible symbol as well as reflecting the themes to be emphasized. While development of both the “logo” and the “tag line” are beyond the scope of this paper, they offer in themselves opportunity for engaged participation by mobile ecosystem constituents. Indeed, co-sponsorship and co-branding by FCC and industry groups of campaign content can serve to build ecosystem buy-in and a common sense of ownership.

PARTNERING ACROSS THE ECOSYSTEM

Although the mobile ecosystem is broad and complex, it is important to obtain buy-in from the various industry segments to leverage their expertise / resources, and to obtain their support for pervasively promoting the campaign content to their customers. We anticipate a key role for the FCC to act as convener, bringing all the key stakeholders to the table to formulate the themes and identify the specific selected threats and safeguards on which to focus.

Key industry associations, such as CTIA, have already made significant efforts in crafting consumer awareness materials, which can serve as a base of content to build upon. With help from other industry groups, such as the Consumer Electronics Association (CEA), the range of coverage can be extended to cover the main segments of the mobile ecosystem.

As noted earlier the mobile ecosystem security landscape is extraordinarily dynamic, and thus the awareness themes and specific guidance must similarly evolve to remain relevant and effective. Criminals and hackers will be as active as developers, manufacturers and operators, all seeking to innovate; the interplay among these participants will likely raise new and unexpected methods and means of attacking consumer interests and undermining confidence in the mobile environment. Thus one of the vital elements for sustaining the awareness and training initiative will be mechanisms for tracking and monitoring threat and risk developments, and then folding suggested guidance for consumers back into the awareness campaign. Academic research teams and nonprofit organizations, in addition to industry groups, might serve as important components of such tracking and monitoring mechanisms.

Finally, the ability to bring media, government and industry recognition and approval to highlight successes is another way the FCC can encourage and empower the stakeholders to remain engaged in the work over an extended time frame.