MOBILE DEVICES (SUCH AS ANDROID, iOS, WINDOWS, AND BLACKBERRY DEVICES) AND MOBILE APPS ARE RAPIDLY BECOMING PART OF EVERYDAY LIFE FOR INDIVIDUAL AND ORGANIZATIONAL USERS IN BOTH DEVELOPED AND DEVELOPING COUNTRIES.

One popular app category is apps that provide cloud-based storage services compatible with a range of devices, including PCs, laptops, and mobile devices. For example, Netskope reports that cloud storage apps such as Google Drive, Amazon CloudDrive, OneDrive, and iCloud were among the top 20 most popular cloud apps during the first half of 2014. Dropbox, another popular cloud storage app, had more than 100 million downloads on the Google Play store at the time of writing.

As with most popular consumer technologies, criminals can exploit vulnerabilities in mobile devices and operating systems or mobile apps to target mobile device and app users. Because of their capability to store vast amounts of user data, cloud storage apps are a potential and attractive target for criminals.

Threats to Mobile Device and Cloud Storage App Users

Gartner predicts that through 2017, 75% of mobile security breaches will be the result of mobile application misconfigurations. By 2017, the focus of mobile breaches will shift to tablets and smartphones from workstations. Through 2015, more than 75% of mobile applications will fail basic security tests.

In May 2014, for example, a significant number of Australian iOS devices were reportedly hijacked and locked for ransom. Subsequent analysis determined that affected users’ iCloud accounts had been compromised. According to various media articles, affected users who didn’t set a passcode prior to the hack had to reset their devices to factory settings, resulting in the erasure of all user data stored on the affected devices.

Mazin Yousif, editor in chief of this magazine, also questioned whether the recent incident in which iTunes customers in 119 countries received U2’s “Songs of Innocence” without their consent suggests that criminals could potentially target iOS mobile device management (MDM). In principle, it isn’t impossible that iOS MDM servers could be compromised, say by a malicious insider, to push malicious or potentially unwanted applications to iOS devices managed by the affected servers. For example, in recent work, Samuel O’Malley and I presented a method that a corrupt insider could use to facilitate data exfiltration from an air-gapped system without using any modified hardware. Such techniques could easily be used to exfiltrate data from cloud servers.

Christoph Stach and Bernhard Mitschang highlighted the implications of poor privacy management approaches. They also pointed out that a vast majority of current mobile apps request access to highly sensitive data and personally identifiable information (PII), such as geographical location and contact data.

In other work, Christian D’Orazio and I proposed a generic process for identifying vulnerabilities and design weaknesses in iOS apps. Using this process, we revealed a previously unknown/
unpublished vulnerability in a widely used Australian Government health-care app that consequently exposes the user’s sensitive data and PII stored on the device.\(^{7}\)

This is, perhaps, not surprising because many mobile apps weren’t designed with user security and privacy in mind, owing to the rush to attract new consumers and accelerate the product’s time to market. Such a situation is somewhat similar to two or three decades ago when published cryptographic protocols were subsequently found to be insecure.\(^{8}\)

Suffice to note that threats to mobile device and cloud storage app users are real and increasingly important because of the increasing amount of user sensitive data and PII stored on and transmitted from mobile devices and cloud storage and other apps (for example, using browsers and apps to upload and download corporate and personal data from mobile devices to cloud storage servers).

Routine Activity Theory Approach
The routine activity theory (RAT), often used to explain criminal events, proposes that crime occurs when a suitable target is in the presence of a motivated offender and is without a capable guardian.\(^{9}\)

Offender motivation is a crucial element of RAT, which assumes that offenders are rational and appropriately resourced actors operating in the context of high-value and poorly protected targets.\(^{10}\) The interaction between potential victims (in our context, mobile device and cloud storage app users), offenders, and situational conditions (for example, opportunities such as devices connecting to free Wi-Fi, and weak guardianship such as poor security hygiene) influences the risk and impact of victimization.

I don’t think many of us want to wake up tomorrow and discover that the data we stored in the cloud was leaked and photos we assumed were private are no longer so. In September 2014, for example, a number of celebrities’ iCloud accounts were reportedly compromised, resulting in the theft of (intimate) photos from these compromised accounts.\(^{11–13}\) Apple subsequently confirmed the incident\(^{14}\):\n
After more than 40 hours of investigation, we have discovered that certain celebrity accounts were compromised by a very targeted attack on user names, passwords and security questions, a practice that has become all too common on the Internet.

Individual mobile cloud users must therefore be vigilant and take measures to protect the data stored on their mobile devices and in the cloud. Such measures should target one or more of the following areas (see Table 1):

- Reducing opportunity (for example, increasing the effort required to offend);
- Enhancing guardianship (for example, increasing the risk of getting caught); and
- Reducing motivation (for example, reducing the rewards of offending).

In summary, security measures shouldn’t lag behind new technology trends. Fortunately, the private sector has enormous incentives for contributing to mobile device/app and cloud security. Now is certainly a good time to get into the business of mobile device/app and cloud security.

WE WELCOME YOUR CONTRIBUTIONS AND ENCOURAGE YOU TO BE PART OF THE MOBILE AND CLOUD SECURITY LANDSCAPE.\(^{16}\)
CLOUD AND THE LAW

From a legal perspective, for example, what are the implications of user data and PII leakage from mobile devices? Should a cloud service provider be responsible for pure economic loss to cloud service users due to its negligent acts? Other areas of interest include the potential surveillance risks faced by mobile cloud storage users, particularly in the aftermath of the revelations by Edward Snowden that the National Security Agency has been conducting wide-scale government surveillance, including those targeting mobile device and cloud users. Therefore, another key question that needs to be examined is, “How do we balance the need for a secure cloud computing ecosystem and the rights of individuals to privacy against the need to protect the society from serious and organized crimes, terrorism, and cyber and national security interests?”

References

Table 1. Suggested areas for improving data protection in mobile devices and cloud storage apps.

<table>
<thead>
<tr>
<th>Security measures</th>
<th>Reduce opportunity</th>
<th>Enhance guardianship</th>
<th>Reduce motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target hardening such as prompt installation of software and hardware patches</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>and antivirus software</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report lost or stolen devices and cybervictimization to appropriate authorities</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Delete data stored on mobile device before disposing of the mobile device and</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>deactivating the account.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete data from cloud accounts before deactivating the account or before the</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>contract expires for corporate cloud users (note that data anonymization and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data deletion are not the same). One could also encrypt the data stored in the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cloud before deleting the encryption key and the encrypted data from the account</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>before deactivating the account or before the contract expires.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avoid visiting websites of dubious repute or downloading unknown apps from</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>third-party app stores</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use device encryption and alphanumeric and nonguessable password for cloud and</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>other accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Use a two-step verification feature offered by cloud services such as Apple 
  | Yes                | Yes                  | No                |


**KIM-KWANG RAYMOND CHOO** is a senior lecturer in the School of Information Technology and Mathematical Science at the University of South Australia. His research interests include cyber and information security and digital forensics. He has published two books, six refereed monographs, nine refereed book chapters, and 101 refereed journal and conference articles. He is the recipient of various awards including a 2010 Australian Capital Territory Pearcey Award, 2009 Fulbright Scholarship, 2008 Australia Day Achievement Medallion and the British Computer Society’s Wilkes Award in 2007. Choo has a PhD in information security from Queensland University of Technology, Australia. Contact him at raymond.choo@fulbrightmail.org or https://sites.google.com/site/raymondchooau.