Article Title: When Context-aware Computing Meets Mobile Security

By University of Waikato's Cyber Security Lab Research Fellow Dr Sivadon (Boom) Chaisiri

People increasingly use mobile devices to access the Internet. An InternetNZ-funded survey conducted by CROW in 2015 shows that 54.6% of mobile users tend to own more than one mobile device and more than 46.4% of them usually use Internet-connected applications on their mobile devices such as social networking (40.7%), Internet browsing (29.9%), and emailing (26.9%). While cyber space and the digital world orbit faster than the Earth, new security threats targeting mobile devices emerge. A security policy has to be well planned to deal with the threats. In this article, I would like to introduce a mobile security solution based on context-aware computing for refining a security policy to adapt to the world-wide-wild cyber space.

An organisation defines a “security policy” as rules, requirements, or a plan on how to protect information systems (including data, networks, and applications) from threats or risks. For example, a company may force you to define and use a password which must contain at least eight characters with a mix of letters, digits, and symbols (such as # @ $ %) and the password must not contain any meaningful words. Such enforcement can protect computers and data from threats such as unauthorised access and identity theft. This example is just one type of security policy, namely a password policy. Other security policies are also important, such as

- Software usage policy to ensure that users install and use only authorised software,
- Web browsing policy to prevent users from browsing unauthorised websites,
- Access control policy to control users’ right to access files (and other computer resources),
- Network firewall policy to block unauthorised incoming/outgoing network traffic,
- Data backup policy to ensure that backup of data has to be done properly,
- Bring-Your-Own-Device (BYOD) policy to control usage of users’ personal devices in the workplace.

Security policies have been enforced in our daily lives, and are being assured that those security policies, along with some security solutions, such as access control, encryption, firewall, and antivirus, can protect our computers, data, and network from being hacked. Those security policies could be our heroes when our computers were disconnected from the rest of the world and when our mobile phone was used for calling and texting only, or when our wristwatch was just a timepiece. But our cyber space is evolving all the time. Now computers exist almost everywhere. Computer-capabilities can be built into anything. Moreover, anything can be connected to the Internet, namely the Internet of Things or IoT, items such as wristwatches, washing machines, heaters, and cars. We can access cyber space anywhere, anytime, even with any appliance.

With our mobile devices, we can access cyber space even on the move. As the number of mobile devices grows, new threats aiming for mobile users’ data increase. TrendLabs revealed that the

number of malicious mobile apps increased from 30,000 in June 2012 to 175,000 in September 2012, just three months! It is clear that the number of threats targeting mobile users will not stop growing.

As with other information security systems, security policies for mobile users can be used to protect against threats aiming for mobile devices and data too. For example, the security policies of a company may enforce mobile users to use a 4-digit-PIN lock screen, connect to a virtual private network (VPN), and turn on mobile phone tracking software (e.g. *Android Device Manager* and *Find My iPhone*) for enhancing security of mobile devices.

Due to the mobility of devices, security policies may not be well adapted to function effectively everywhere, every time, and in every environment that we are associated with. In other words, such security policies are obsolete due to dynamic changes in time, location and environments surrounding mobile users (e.g. people around them) and the users' activities (e.g. doing exercises, having a meeting, and sleeping). Generally, security policies are inflexible and slow to adapt to the dynamic nature of mobile environments and that can have an impact on security postures. For example, suppose an access control policy allows us to have full access to a customer database such that you can view and modify the database at our company. What if we have to access the database in other places? At a customer's location, we should access information inside the database related to this customer only. At a coffee shop where we are having a meeting with our sales team, we should only view the whole database but should not be able to modify it; however, at lunchtime when the coffee shop is always crowded, we may not have access to the database although the meeting with the sales team has to continue (suppose the meeting cannot be rescheduled). When we are back home, we may want to continue our work related to the database but only with the *view-only* access. Finally, when we sleep and dream about the last meeting, we should not have access to the database at all (as we do not need the database when sleeping).

Context-aware computing, that has been studied and developed for more than a decade, is a promising solution for dealing with threats targeting mobile technologies. With context-aware computing, a computer or a mobile device can sense *context*, and it can then match appropriate processes to adapt to the context. Context can be location, time, activities, environmental conditions (e.g. temperature, humidity, light intensity, and noise level). Context-aware computing can be applied to several applications such as mobile computing, entertainment, manufacture, healthcare, transportation, and also *mobile security*.

When context-aware computing meets mobile security, we will obtain adaptive security policies that can be adjusted to context associated with the mobile users. For example, our mobile device may be automatically unlocked when we are at home (supposing our parents or spouse will not violate our privacy). The device switches the screen to a 4-digit-PIN lock screen when we work in our office building. When we leave the office, the screen is switched to a 6-digit-PIN lock screen and an encrypted VPN connection is established for connecting to the Internet while a firewall with strict traffic blocking rules is used. When we walk at night or in crowded areas, our device is locked with a strong password. Whenever the device is lost or stolen (e.g. the device being away

from our hands by a long distance or for longer than several hours), all data inside the device will be automatically wiped out to protect access to our device and confidential data.

Context-aware computing for security, called *context-aware security*, requires sensors to detect or to be aware of context. Context can be detected by sensors built into a mobile device such as clock/timer, position sensors (e.g. GPS), microphone, camera, biometric sensors, and kinaesthetic sensors. Moreover, we can combine data from the sensors in the mobile device with other data from external sensors and Internet services such as CCTV, weather forecasting service, tweets from Twitter, and appointment service (such as Google Calendar and Facebook events). A combination of data obtained from these sensors can help us define a fine-grained security policy.

Several current and future applications can gain benefits from this context-aware security such as parental control, BYOD, IoT, and 5G networks. Research on context-aware security is still ongoing. Hopefully, context-aware security will be soon integrated into mobile devices like smartphones and mobile gadgets. Consequently, our lives will be more convenient with mobile technologies, but appropriate security policies will be automatically refined and adjusted to changes according to context, time and space, or other things which can be sensed.

If you are interested in context-aware security, read our recent publication: "*From Reactionary to Proactive Security: Context-Aware Security Policy Management and Optimization Under Uncertainty"* authored by myself (Sivadon Chaisiri) and Dr Ryan Ko. This was recently presented at the IEEE TrustCom 2016 (an *A*-ranked conference by CORE) held in Tianjin, China.