رسیدگی به حوادث سامانه هوشمند تلفن همراه

اخیرا شاهد تغییر مداوم تکنولوژی از کامپیوترهای رومیزی به دستگاه‌های تلفن همراه بوده‌ایم. محبوبیت تلفن‌های هوشمند همراه به عنوان ابزاری پرکاربرد و چند منظوره که در سطوح مختلف جامعه نفوذ پیدا کرده، مدام در حال افزایش است. تلفن‌های هوشمند همراه به دلیل چند منظوره بودن برای انجام اموری پرداخت قبوض، خرید آنلاین، مدیریت حساب مالی، شبکه‌های اجتماعی و ایمیل، به اطلاعات حساس دسترسی دارند و می‌توانند فرصت مناسبی برای مجرمان سایبری فراهم نمایند. شبیه تمام تکنولوژی‌های دیگر، نقص‌های امنیتی تلفن‌های هوشمند همراه، افراد و سازمان‌ها را در معرض خطرات جدی قرار می‌دهد. دستگاه‌های غیرامن، برنامه‌های کاربردی دارای نشتی و آسیب‌پذیری، فروش آسیب‌پذیری به صورت سلاحی علیه امنیت و افزایش نرخ توسعه بدافزارهای پیشرفته موبایل، همگی تهدیداتی جدی برای اکوسیستم سامانه هوشمند تلفن همراه محسوب می‌شوند. مجموعه این اکوسیستم ناامن چگونگی تفکر در مورد پاسخ به حوادث موبایل را شکل می‌دهد و سازمان‌های خصوصی و دولتی را ملزم به پشتیبانی از استراتژی پاسخ به حوادث موبایل می‌نماید. پاسخ به حوادث موبایل به دلایلی که بیان خواهد شد، متفاوت از پاسخ به حوادث کامپیوتر شخصی و لپ‌تاپ است از اینرو در فصل اول این کارگاه فرآیند رسیدگی به حوادث تلفن هوشمند همراه، انوع حوادث موبایل، ابزارهای مورد نیاز برای رسیدگی به حوادث بررسی خواهد شد و برای درک بیشتر به مطالعه موردی پاسخ به حوادث تلفن هوشمند همراه، پرداخته می‌شود.

Investigation into Mobile Incident Handling

Recently, the technology regarding desktop computers has been increasingly shifted towards smartphones. Besides, the popularity of smartphones has caused revolutionary development and increasing deployment of smartphones, allowing users to use them as essentials and multi-purpose devices. These multi-purpose devices allow users to have the advantage of using their email accounts, pay bills, online shopping, financial account management, social media, and etc. On the other side of scale, the availability of these information on smartphones provides a sharp increase of the possibility of malicious activities and a prolific environment for exploitation by cybercriminals. Like other technologies, smartphones have their own security flaws which expose the individual users and enterprise to risks. Additionally, unsecure devices, leaky applications, critical vulnerabilities, selling vulnerabilities as weapons against security, and increasing of development of mobile malwares have been considered as critical threats for the smartphones ecosystem. This kind of unsecure ecosystem

shapes the mindset about mobile incident responses and it is essential for organization, enterprise, and governments to support the strategies of responses to smartphones incidents. The unique features of smartphones do present certain challenges when responding to a mobile incident that makes mobile incident response different from traditional network or computer-based incident response for a number of provided reasons. Therefore, on the first section of this workshop, mobile incident response challenges, mobile incident process, mobile incident response tools, case study and security requirements will be discussed.