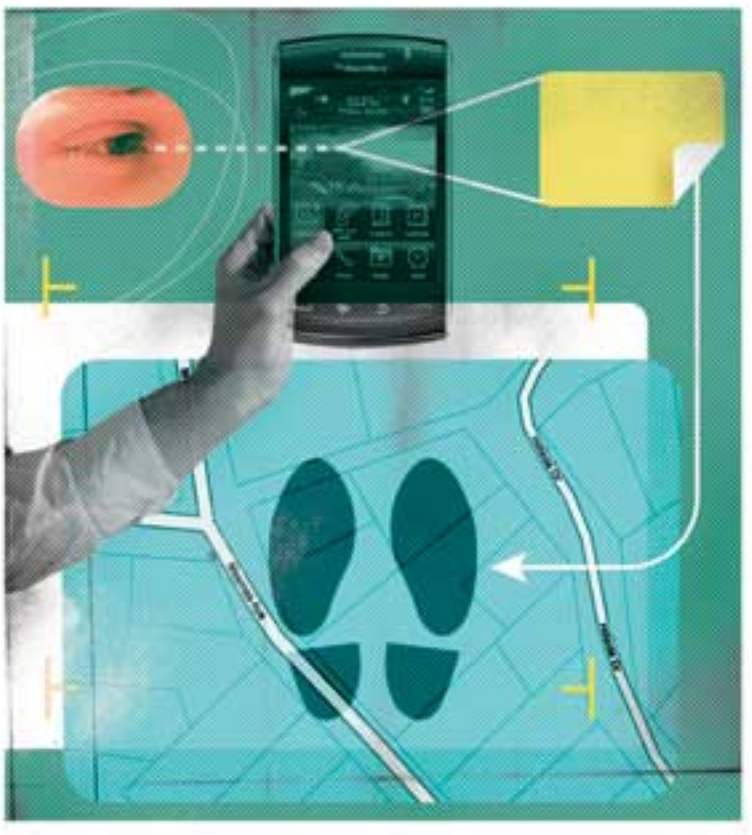
Security Alert

ဓာတ်ပုံတွေက ပြောတဲ့ ကိုယ့်အကြောင်း

ဒီအချိန်ကတော့ တကယ့်ကို ထူးခြားတဲ့အချိန်ပဲ ဖြစ်ပါတယ်။ iPhone ရဲ့ camera ကိုသုံးပြီး ဓာတ်ပုံရိုက်ပါ။ Twitpic ပေါ် ကို ဓာတ်ပုံတွေ upload တင်ပြီး twitter ပေါ် ကတစ်ဆင့်လည်း share လုပ်နိုင်ပါသေးတယ်။

ပုံတွေတင်တဲ့အခါ ၇၅ သန်းရှိတဲ့ twitter သုံးစွဲသူတွေဟာ ကိုယ်နဲ့ ကိုယ့်ရဲ့ကလေးဘယ်နေရာမှာ ရှိတယ်ဆိုတဲ့ နေရာအတိအကျကို သိနိုင်ပါလိမ့်မယ်။ Digital photo တွေဟာ camera ကတစ်ဆင့်ထုတ်တဲ့ EXIF data လို့ခေါ်တဲ့ information ဒုနဲ့ဒေးတွေကို အလိုအလျောက် သိမ်းဆည်းပေးပါတယ်။ Data အများစုကတော့ အန္တရာယ်မရှိပေမယ့် twitter ပေါ်မှာတင်ထားတဲ့ ဓာတ်ပုံအားလုံးရဲ့ ၃ ရာခိုင်နှုန်းမှာ location နဲ့ ပတ်သက်တဲ့ data တွေပါနေတယ်ဆိုပြီး New York မှာ ပြုလုပ်တဲ့ security conference မှာ ဆိုထားပါတယ်။ ဒီအရေအတွက်ဟာလည်း တဖြည်းဖြည်းနဲ့ တိုးလာနေတယ်လို့ ဆိုပါတယ်။ ဒီ data တွေကိုကြည့်နေတဲ့ web ပေါ်က မည်သူမဆို ဓာတ်ပုံကိုရိုက်ထားတဲ့သူက ဘယ်နေရာမှာ ရပ်နေခဲ့သလဲဆိုတာ သိတယ်လို့ ပြောပါတယ်။ ဒါဟာ personal privacy ကို ချိုးဖောက်တာမျိုးဖြစ်ပါတယ်။



Mobile phone က ပုံတွေမှာပါတဲ့ geotagging data တွေက ကိုယ်တယ်နေရာမှာ ရောက်နေသလဲဆိုတာကို သူစိမ်းတွေ သိစေပါတယ်။

EXIF Data နဲ့ Geotagging

ဒီ Exchangeable Image File (EXIF) format ဟာ ပုံမှန် JPG နဲ့ TIFF image file တွေမှာ meta data တွေ ထည့်ပေးပါတယ်။ ဓာတ်ပုံရဲ့ thumbnail ပုံနဲ့အတူ EXIF data မှာ aparture၊ shutter speed၊ focal length၊ metering mode ၊ ISO setting နဲ့ final printed image တွေ အဆင်ပြေပြေဆောင်ရွက်နိုင်ဖို့ printer ကို ထောက်ပံ့ပေးထားတဲ့ အချက်စတဲ့ အသေးစိတ်အချက်အလက်တွေကို သိမ်းဆည်းထားပေးပါတယ်။ Camera ရဲ့ ထုတ်လုပ်သူ၊ registration number နဲ့ location data တွေစတဲ့ တခြားအချက်အလက်တွေကိုလည်း EXIF မှာ ထည့်သွင်းထားဖို့ နေရာရှိပါသေးတယ်။

Geotagging ဆိုတာ ပုံရဲ့ EXIF data အတွင်းမှာရှိတဲ့ လောင်ဂျီတွဒ်နဲ့ လတ္တီတွဒ် data တွေကို သိမ်းပေးတဲ့ process ပဲ ဖြစ်ပါတယ်။ ဒီအချက်တွေဟာ ပုံနဲ့ဓာတ်ပုံရိုက်ကူးသူရဲ့ google earth လို mapping service မျိုးကနေ geo location တွေကို တွဲဖက်ပေးပါတယ်။

Digital camera အဟောင်းတွေအတွက် ပုံမှာ location data တွေ ထည့်ဖို့ဆိုရင် ရှုပ်ထွေးတဲ့တန်ဆာပလာတွေလိုအပ်ပါတယ်။ Camera ကို stand alone navigation device၊ ဒါမှမဟုတ် mobile phone လို GPS receiver နဲ့ ချိတ်ဆက်ဖို့

cable တစ်ခုကို တွဲဆက်ရပါမယ်။ ဒါပေမဲ့ digital camera အမျိုးအစားအသစ် တော်တော်များများနဲ့ mobile phone camera တွေမှာ built-in GPS receiver တွေ ပါဝင်ပါတယ်။ ဒီလို device အသစ်တွေမှာ geotagging feature တွေကို ပေါင်းစပ်ထားတာဖြစ်ပြီး ကိုယ့်ရဲ့ EXIF file တွေမှာ လတ္တီတွဒ်၊ လောင်ဂျီတွဒ်၊ အချိန်နဲ့ ပင်လယ်ရေမျက်နှာပြင်ထက် အမြင့် စတဲ့အချက်တွေကိုပါ သိမ်းဆည်းပေးနိုင်ပါတယ်။

ICanStalkU.com

Geotagging related privacy ပြဿနာတွေကို အလေးပေးပြောရမယ်ဆိုရင် Jackson နဲ့ Larry Pesce ဆိုသူတွေဟာ geotagged ပုံတွေတင်ထားတဲ့ tweeter တွေဆီကို respond ပြန်ဖို့အတွက် ICanStalkU ဆိုတဲ့ twitter user name ကိုယူသုံးထားပါတယ်။ Twitter က ဒီ account ကို ပိတ်ခဲ့ပေမယ့် user တွေကို ပညာပေးဖို့ လိုအပ်ချက်အတွက်လို့ ငြင်းဆိုပြီးတဲ့နောက်မှာ Jackson ကို ပြန်ဝင်ခွင့်ပြုခဲ့ပါတယ်။ ဒီ message ကို သိစေဖို့ လည်း သူဟာ *ICanStalkU.com* ဆိုတဲ့ website ကို လွှင့်တင်ခဲ့ပါတယ်။

ICanStalkU ဟာ MobyPicture၊ SexyPeek၊ Twitter နဲ့ Yfrog တို့မှ ပုံပေါင်း ၂၀,၀၀၀ ကျော်ကို နှေ့စဉ်ဖယ်ပစ်ဖို့ Perl script ကိုသုံးပါတယ်။ ပြီးတဲ့နောက်မှာ "I am currently nearby ..." ဆိုတဲ့ message နဲ့အတူ ပုံတွေကို ပြန်တင်ပေးပြီး အဲဒီပုံတွေမှာ လမ်းလိပ်စာ၊ လတ္တီတွဒ်၊ လောင်ဂျီတွဒ် ၊ မြို့၊ ပြည်နယ်အချက်အလက်တွေကို ထည့်သွင်းပေးထားပါတယ်။ ICanStalkU entry တစ်ခုချင်းစီဟာ google ၊ မူလ tweet နဲ့ မူလဓာတ်ပုံပေါ်မှာ map လုပ်ထားတဲ့ location တွေကိုလည်း ပြသပေးပါတယ်။

နောက်ထပ် site တစ်ခုဖြစ်တဲ့ *PleaseRobMe.com* (အခုတော့ ပိတ်ထားပါတယ်) ဟာ online ပေါ်တင်ထားတဲ့ personal data တွေကို လျှော့ချဖို့ Foursquare နဲ့ twitter တို့ကနေ data တွေကိုအသုံးပြုခဲ့ပါတယ်။ Project ရဲ့ နောက်ကွယ်က သုတေသနပညာရှင်တွေကတော့ ဒီ project ဆက်မလုပ်ခင် ရရှိထားတဲ့ feedback တွေကို ပြန်လည်သုံးသပ်နေတယ်လို့ ဆိုပါတယ်။

Jackson ရဲ့ security conference presentation (*find.pcworld.com/70798*) မှာ ဓာတ်ပုံထဲက လူတစ်ယောက်ရဲ့ အကြောင်း အသေးစိတ်အချက်အလက်တွေကို ဘယ်လို တွေ့ခဲ့တယ်ဆိုတာ ပြောပြခဲ့ပါတယ်။ Geotagging data တွေကို အသုံးပြုပြီး Jackson ဟာ google earth ပေါ်မှာ အဲဒီလူရဲ့ အိမ်ကိုနေရာ ချကြည့်ခဲ့ပါတယ်။ ပြီးတော့ ဓာတ်ပုံရိုက်ယူထားတဲ့ အိမ်နဲ့ ပတ်သက်တဲ့နာမည်ကိုလည်း တွေ့သွားခဲ့ပါတယ်။ အဲဒီကနေ မွေးနေ့၊ အိမ်ထောင်ရေးအခြေအနေနဲ့ သူငယ်ချင်းတွေ စတဲ့ အချက်တွေဖော်ပြထားတဲ့ facebook account ဆီကို ဦးတည်သွားတော့တာပါပဲ။ Facebook page မှာဖော်ပြထားတဲ့ second user name ကနေ second twitter account ဆီကို ရောက်သွားပြီး ဒီလိုနဲ့ ရှေ့ဆက်တွေ့ရှိသွားတာပဲ ဖြစ်ပါတယ်။

တချို့လူတွေကတော့ သူတို့နဲ့လုံးဝမသိတဲ့သူတွေနဲ့ real time location data တွေ share လုပ်ရတာ ကိစ္စမရှိပါဘူးလို့ ဆိုပါတယ်။ ဒါပေမဲ့ တချို့လူတွေဟာ သူစိမ်းတစ်ယောက်က သူတို့ရဲ့နေရာကို သိသွားတာမျိုးကို သဘောမကျကြပါဘူး။ Smartphone နဲ့ camera တွေမှာ photo geotagging feature ကို turn off လုပ်ထားလို့သာ တော်သေးတာပေါ့လို့ ဆိုကြပါတယ်။

Phone နဲ့ ပတ်သက်တဲ့ ကုစားချက်

iPhone မှာဆိုရင် Foursquare မှာလိုပဲ geolocation app တွေအားလုံးလို disable လုပ်ပြီး geotagging ကို block လုပ်ထားနိုင်ပါတယ်။ ဒီလိုလုပ်ဖို့ဆိုရင် setting >> general ကိုသွားပြီး Location service setting ကို off အနေအထားကို toggle လုပ်ပြီးပြောင်းပါ။ iOS4 မှာ သက်ဆိုင်ရာ app တွေအတွက် location service တွေကို disable လုပ်နိုင်ပါတယ်။ iOS4 ကိုမသုံးဘူးဆိုရင် phone တစ်ခုလုံးအတွက် location service တွေကို ပိတ်မယ့်အစား local warning တွေကို reset လုပ်ထားနိုင်ပါတယ်။ Setting ကို သွားပြီး reset ကို tap လုပ်ပါ။ ပြီးရင် 'Reset Location Warning' ကို select လုပ်ပါ။ Camera ကိုဖွင့်ပြီး 'Ask on first use' မေးခွန်းမှာ no လို့ထည့်ထားပါ။ နောက်တစ်ကြိမ်ဖွင့်တဲ့အခါမှာ app တစ်ခုချင်းစီကို 'allow'၊ ဒါမှမဟုတ် 'disallow' လုပ်နိုင်ပါတယ်။

Android phone တွေမှာဆိုရင်တော့ GPS ကို ပိတ်ထားတာက location based app တွေ အားလုံးကိုပိတ်ပြီးသားဖြစ်စေပါတယ်။ အဲဒီအစား camera app ကိုဖွင့်ပြီး ဘယ်ဘက်ခြမ်း menu က 'location and security' အောက်မှာ GPS ကို disable လုပ်ပါ။ ပြန်စစ်မယ်ဆိုရင် camera app ကိုဖွင့်ပြီး ဘယ်ဘက်က menu ကို ဖွင့်ပါ။ 'Store location' က disable အနေအထားမှာ ရှိနေရပါမယ်။ RIM balckberry မှာတော့ camera ထဲက feature ကို disable လုပ်ရတာ လွယ်ပါတယ်။ Menu key ကိုနှိပ်ပြီး disable GPS ကို ရွေးချယ်ပါ။ အတည်ပြုဖို့ yes ကို ရွေးချယ်ပါ။

Black Hat ထုတ်ဖော်မှုကို တုံ့ပြန်လိုက်တဲ့ Adobe

Adobe ဟာ ပြင်းထန်စွာတိုက်ခိုက်ခံရပြီဆိုတာ ဇူလိုင်လက Las Vegas မှာလုပ်ခဲ့တဲ့ Black Hat USA 2010 security conference မှာ ဆွေးနွေးခဲ့ပြီး အရေးပေါ် update တွေ လုပ်ဖို့ပြောခဲ့ပါတယ်။ အဲဒီအချိန်မှာ Microsoft ကလည်း သူတို့ရဲ့ monthly fix ကို ပြုလုပ်ခဲ့ပြီး ဒီတစ်ကြိမ်မှာတော့ ချို့ယွင်းချက် ၁၄ ခု ကို ပြန်လည်ပြင်ဆင်ခဲ့တာ ဖြစ်ပါတယ်။

ပုံမှန်မဟုတ်တဲ့ Adobe ရဲ့ ထုတ်ပြန်ချက်

ဩဂုတ် ၁၉ ရက်မှာ Adobe ဟာ update တွေထုတ်ပြန်ခဲ့ပြီး နောက်ထပ်ပြင်ဆင်မှုတွေကို အောက်တိုဘာ ၁၂ ရက်လောက်မှာ ထုတ်ပြန်ခဲ့ပါတယ်။ အဲဒီနှစ်နွေရာသီမှာလုပ်တဲ့ Black Hat USA 2010 security conference မှာ ထုတ်ပြန်ခဲ့တဲ့ အမှားတွေကိုပြင်ဆင်ထားတဲ့ update တွေမှာ Adobe Flash Player အတွက် ပြင်ဆင်မှုတွေလည်း ပါဝင်ပါတယ်။ ဖြစ်ပေါ်ခဲ့တဲ့ ပြဿနာတွေဟာ Windows ၊ Mac နဲ့ Unix တို့အတွက် Adobe reader 9.3.3 နဲ့ အရင် version တွေ ၊ Windows နဲ့ Mac အတွက် Acrobat 9.3.3 နဲ့ အရင် version တွေ၊ Windows ၊ Mac ၊ Linux နဲ့ Solaris တို့အတွက် Flash Player 10.1.53.54 နဲ့ အစောပိုင်း version တွေအပြင် Windows ၊ Mac နဲ့ Linux အတွက် AIR 2.0.2.12610 စတဲ့ app တွေကိုပါ ထိခိုက်မှုတွေ ဖြစ်စေပါတယ်။ ကုမ္ပဏီက Adobe Reader နဲ့ Acrobat ကို တိုက်ခိုက်တဲ့သူတွေက အဓိကလုပ်ထားတာဆိုပြီး သတ်မှတ်ပါတယ်။ အကြောင်းကတော့ app တွေကို crash ဖြစ်စေပြီး attacker တွေကိုလည်း system ထဲကိုဝင်ပြီး control လုပ်ခွင့်တောင် ပေးထားနိုင်တဲ့အတွက်ပဲ ဖြစ်ပါတယ်။ Adobe Flash Player နဲ့ AIR မှာရှိတဲ့အမှားတွေအတွက် update တွေဟာ attacker တွေ remote execution စွမ်းရည်ရသွားစေနိုင်တဲ့ program တွေရဲ့ memory handling အပိုင်းနဲ့ ဆောင်ချောက် မရှိဘူးထင်ရတဲ့ webpage တွေကို click လုပ်တဲ့အခါမှာ system ကို control လုပ်နိုင်တဲ့ ၊ ဒါမှမဟုတ် user ကို information တွေပြအောင် လှည့်ဖြားနိုင်တဲ့ clickjacking ဖြစ်သွားစေနိုင်တာတွေကို ပြင်ဆင်ခဲ့ပါတယ်။ ပုံမှန်အတိုင်း automatic update check တွေကိုသုံးပြီး PC ရဲ့ Adobe Reader ၊ Acrobat ၊ Flash Player နဲ့ AIR စတာတွေရဲ့ နောက်ဆုံး version တွေကို update လုပ်ထားသင့်ပါတယ်။

Microsoft ရဲ့ ပြင်ဆက်ချက်များ

Microsoft ရဲ့ ပြင်ဆင်မှုတွေမှာ security update ၁၄ ခု ပါဝင်ပြီး ၆ ခုကတော့ အရေးကြီးတဲ့အဆင့်မှာ ရှိကာ ကျန်တဲ့ ၈ ခုကတော့ critical ပဲ ဖြစ်ပါတယ်။ Windows XP ၊ Vista ၊ Wins 7 ၊ Server 2003 ၊ Server 2008 နဲ့ Server 2008 R2 စတဲ့ version တွေအားလုံးအတွက် update လုပ်ခဲ့ပါတယ်။ Security update ၁၄ ခုမှာ ၇ ခုကတော့ Microsoft က သူ့ windows အတွက်ပြင်ဆင်တာ ဖြစ်ပါတယ်။ အန္တရာယ်ရှိတဲ့ code တွေပါဝင်တဲ့ website တွေနဲ့ link တွေကို ဖွင့်လိုက်တဲ့အခါမှာ attacker တွေ ဝင်ရောက်နိုင်ပါတယ်။ ဒါမှမဟုတ် ဝင်ရောက်မယ့်သူဟာ PC ကို physical access လုပ်မယ်ဆိုရင် နောက်ထပ် access လုပ်ခွင့်တွေရဖို့ မရိုးသားတဲ့ program တွေ run နိုင်ပါတယ်။ ကျန်ရှိနေတဲ့ update တွေဟာ Microsoft XML Core Services (programmer တွေအတွက် tool တစ်ခု) ၊ Windows Media Playen Internet Explorer ၊ Windows Server နဲ့ Microsoft Office အပြင် .Net framework မှာ ရှိတဲ့ အားနည်းချက်တစ်ခု စတာတွေမှာရှိတဲ့ ပြဿနာတွေနဲ့ ပတ်သက်တဲ့ update တွေ ဖြစ်ပါတယ်။ အထူးပြုလုပ်ထားတဲ့ link ၊ website ၊ Excel file ၊ ဒါမှမဟုတ် media file တွေထဲက တစ်ခုခုကိုဖွင့်လိုက်ပြီဆိုရင် ဒီ security အပေါက်တွေက တစ်ဆင့် attacker တွေ ဝင်ရောက်နိုင်ပါတယ်။ ဒီလို link မျိုးဟာ system မှာ code တွေ run နိုင်ပြီး attacker တွေက PC ကို remote access လုပ်ကာ ထိန်းချုပ်စေနိုင်မှာဖြစ်ပါတယ်။

စောကလျာအေး