

Sammanfattning

Inom en snar framtid kommer antalet mobila terminaler med stöd för utbytbara applikationer att öka kraftigt. Detta innebär att mobila terminaler som till exempel våra mobiltelefoner kommer att kunna göra mycket mer än att upprätta samtal. Vårt mål med denna uppsats är att utreda möjligheten att skapa och sprida applikationer som verkar på ett skadligt sätt för användaren. Vi begränsar oss till applikationer för de mobila terminaler som stödjer javaplattformen. Då utveckling av applikationer för dessa enheter görs tillgänglig för tredjepartsutvecklare kommer säkerheten att sättas på prov. Det är viktigt att säkerheten mot skadliga applikationer är god eftersom mobila terminaler och särskilt mobiltelefoner är produkter som riktar sig mot en mycket stor grupp användare, en grupp för vilken tekniska lösningar och säkerhetsfrågor bör vara så transparenta som möjligt.

Nödvändig kunskap för att kunna genomföra uppsatsen har vi till stor del hämtat från Internet och specifikationer i form av digitala dokument eftersom ämnet är så nytt att det ännu inte finns böcker som behandlar det. Vi har studerat bakgrunden till javaplattformen i mobila terminaler, dess säkerhetsmodell samt områden där olika angrepp kan tänkas gå att genomföra. Därefter har vi genomfört en analys av möjligheterna att skapa och sprida skadlig kod inom dessa områden samt gjort ett antal tester.

Vi har kommit fram till att javaplattformen i mobila terminaler är säker i den omfattning som krävs av dess säkerhetsmodell. Säkerhetsbrister kan ändå uppstå i olika mobila terminaler eftersom tillverkarna själva implementerar javaplattformen i dem. Flertalet av de få brister i säkerheten vi funnit är inte specifika för mobila enheter med stöd för javaplattformen, utan är allmänna angrepp som går att utnyttja även på andra plattformar och enheter.

Malicious code with Java in mobile phones

Abstract

In the nearest future, the number of mobile devices supporting interchangeable applications will increase. Mobile devices, like our mobile phones, will be able to do more than setting up voice calls. Our goal with this Bachelor project is to investigate the possibility to create and distribute applications that act malicious to users. We will only concern devices implementing the Java platform. When third party developers create applications for mobile devices, the security of the Java platform will be tested. It is important that the occurrences of malicious applications are kept at a minimum because mobile devices such as mobile phones are directed towards a huge group of consumers. This is a group for which issues about technique and security should be as transparent as possible.

We have collected necessary knowledge mainly from the Internet and various specifications in digital format. These sources were used since the subject is relatively new and no books treat it yet. We have studied the background of the Java platform in mobile devices, its security model and areas where potential attacks could be made. After that, analyses of the possibilities to create and spread malicious code through these areas are made and some tests are conducted.

We have reached the conclusion that the Java platform in mobile devices is safe in the scope of its security model. We are not, however, saying that security flaws cannot appear when the Java platform is implemented erroneously in specific devices. Most of the security flaws we discovered are not specific for mobile devices supporting the Java platform, but are general and applicable to other platforms and devices as well.