Tvåfaktorsautentisering i smarta telefoner: Implementationer och attacker

Dagens smartphones har mycket gemensamt med en vanlig persondator. Med dessa kraftfulla telefoner kommer dock inte endast fördelar. Skadlig kod, eller virus, har även möjlighet att drabba smartphones. Ett populärt mål för de kriminella som skriver skadlig kod till smartphones är inloggningsuppgifter, och mer specifikt inloggningsuppgifter till finansiella tjänster som exempelvis internetbank. I detta exjobb analyseras tre olika tvåfaktorsautentiseringsmetoder som utnyttjas på smartphones och deras möjligheter att motstå skadlig kod och andra attacker.

Det traditionella sättet att autentisera användare vid inloggning till olika tjänster har under en längre tid endast bestått av att verifiera deras användarnamn och lösenord. Detta har visat sig vara mindre bra då denna användarinformation lätt kan läcka till följd av t.ex. en hackerattack. Som en förbättring så kan man införa ytterligare ett lager av säkerhet för att förhindra obehöriga att få tillgång till andras användarkonton. Ett exempel är att personen som vill logga in även får ett SMS skickat till sin mobiltelefon innehållande en kod som även den måste matas in för att inloggningen ska fullföljas. Detta är en s.k. tvåfaktorsautentiseringsmetod där innehållet i SMS:et står för den andra faktorn och användarnamn och lösenord står för den första.

Metoden med autentisering via SMS kallas för mTAN och är en av de tre metoderna som utvärderas i exjobbet tillsammans med TOTP och Mobilt BankID. En implementation av metoden TOTP (Time-based One-time Password Algorithm) som Google står bakom låter användarens smartphone generera koder som är baserade på förfluten tid samt en hemlig delad nyckel. Tjänsten Mobilt BankID som har blivit ett populärt sätt att autentisera sig på svenska webbsidor är även det en säker metod som förlitar sig på en infrastruktur som redan används på internet idag för att intyga olika parters identiteter, en s.k. PKI (Public Key Infrastructure).

För att få en förståelse för hur en attack med skadlig kod kan gå till mot mTAN-metoden så analyseras en s.k. trojan som är byggd för Android i exjobbet. En trojan är ett program som utger sig för att vara något annat än det egentligen är. I detta fall utger den sig för att vara en säkerhetsapp för inloggning till Facebook, men i själva verket så är det sanna syftet att stjäla kontaktuppgifter och SMS-innehåll från användaren genom att köras i bakgrunden på telefonen. Trojanen analyseras i exjobbet genom att bl.a. köra den i en simulator där dess funktionalitet kan observeras och kontrolleras. Försök att styra trojanen till att utföra diverse operationer, som t.ex. skicka hela kontaktlistan till en tredjepart eller vidarebefordra inkommande SMS till densamma, lyckas och redovisas i rapporten. Med andra ord är det möjligt för cybertjuvar att komma över koder som skickas via SMS i syfte för inloggning.

I exjobbet visar det sig att autentiseringslösningar via SMS, s.k. mTAN, är sårbara mot attacker och ej bör användas om det är möjligt. Det existerar dock andra, avsevärt säkrare, tvåfaktorsautentiseringsmetoder byggda för smartphones som TOTP och Mobilt BankID. Tvåfaktorsautentisering via SMS är en gammal metod som fungerade väl när mobiltelefonerna ej var så avancerade som de är idag. Den säkerhetsmedvetne användaren bör alltid använda tvåfaktorsautentisering om det erbjuds, och helst föredra en TOTP-lösning eller Mobilt BankID.

Av: Christofer Ericson