Tweede Toets Security

5 november 2018, 8.30 – 10.30, Educ-α.

Motiveer je antwoorden *kort*! Stel geen vragen over deze toets; als je een vraag niet duidelijk vindt, schrijf dan op hoe je de vraag interpreteert en beantwoord de vraag zoals je hem begrijpt. Vragen 1 t/m3 zijn elk 3pt en vragen 4 t/m 6 elk 2. Maak vragen 1 en 2 op de voorkant, vragen 3 en 4 op pagina 2 en vragen 5 en 6 op pagina 3. **Answer question 4 through 6 in English!**

1. **RSA Weetjes:** (a) Door wie is RSA uitgevonden en wanneer?
   (b) Welke sleutellengtes kun je veilig gebruiken en welke niet?
   (c) Beschrijf de sleutelgeneratie voor k-bits RSA en zeg hoe lang de gebruikte getallen zijn.

2. **Sign-Copy-Paste:** Voor het ondertekenen van een bericht met RSA wordt doorgaans eerst een hash van het bericht berekend.
   (a) Waarom wordt dit gedaan? (Noem twee of drie redenen.)
   (b) Wat is *Sign-Copy-Paste* en welke eigenschap van Hashfuncties beschermt ertegen?
   (c) Kan een hashfunctie van 160 bits voldoende beschering bieden tegen deze aanval?

3. **Gegenereerde groep:** In deze vraag is p een (groot) priemgetal en $g \in \mathbb{Z}_p^*$ heeft orde q.
   (a) Noem G de verzameling van alle *machten van* g. Hoeveel elementen heeft G?
   (b) Bewijs dat elke $x \in G$ een inverse heeft, en dat $x^{-1} \in G$.
   (c) Gegeven een $x \in G$, is het mogelijk de i te vinden waarvoor $g^i = x$? Leg kort uit!

4. **Exploits:** Assume that you have one physical machine available that you want to use to run a web server (`apache2`) and a mail server (`qmail`). Consider the following scenarios:
   (a) Both the `apache2` process and the `qmail` process run as user `root` natively on a Linux system.
   (b) The `apache2` process runs as user `web`, the `qmail` process runs as user `mail`. Each of those two users has `read/write` access only to the files that it needs to have access to in order to function (e.g., `mail` has read/write access to mails; `web` has read access to html files that it serves).
   Assume that an attacker has an exploit against the web server that gives a shell with the permissions of the web server (i.e., as the user that is running apache2). The target of the attacker is to access mails stored by the qmail process.
   For each of the scenarios above, explain what the attacker needs to do in order to obtain these mails and what additional exploits (if any) are required.

5. **PAM Configuration:** Consider the PAM module `pam_fprint.so`, which allows authentication by fingerprint and consider the following configuration in `/etc/pam.d/login`:
   ```
   auth sufficient pam_fprint.so
   auth sufficient pam_unix.so
   auth required   pam_deny.so
   ```
   (a) Briefly explain what authentication policy this configuration enforces.
   (b) Is the policy described above more restrictive or less restrictive than the policy enforced by the following configuration:
   ```
   auth required pam_unix.so
   ```
   Explain your answer.

6. **Flooding:** Denial-of-service (DoS) attack can be referred to as an explicit attempt by attackers to prevent legitimate use of a service. One technique which can be used to carry out such a DoS attack on a network is **flooding**.
   State and briefly (2–3 lines per item) describe two types of DoS-based flooding attacks.