Tentti S-38.153 Tietoliikenteen tietoturva
Exam S-38.153 Security of Communication Protocols

11.5.2005 Hall S1 9-12

Put your name, student number, course code and date to below and each exercise paper. This helps you to receive your credits in fast and reliable manner. Answers are accpeted in Finnish, Swedish or in English. Answers are judged based on their quality and clarity. A short and down to the fact answer will get better points than a excursive one. You may explain things further but beware that errors may lower your points (even if they are in extra matter).

Nimi/Name:			
Opnro/Studid		Osasto/Department	

1. Tarkastele seuraavia tapauksia: perustele lyhyesti mitä tekisit tilanteen ratkaisemiseksi ja miksi (2 p/tapaus).
   Evaluate following cases: what would you do to resolve situation and why? (2 p/case)
   (a) Internet-kauppapaikkaa pyörittävälle palvelimelle on murtauduttu ja todennäköisesti saatu pääkäyttäjän oikeudet. Järjestelmän ajaminen alas aiheuttaa noin 50.000 € kustannukset ennen kuin varajärjestelmä on saatu käyttöön.
   Server running internet shop has been compromised and most probably the intruder has root user rights. Shutting down system causes 50,000 € expences before backup system is online.
   (b) Aiemmin tuntematonta haavoittuvuutta käyttävä mato leviää saastuttaen web-palvelimia ja web-selaimien välityksellä päätelaitteita jotka vastavuoroisesti saastuttavat web-palvelimia. Yrityksessä on tilallista suodatusta käyttävä palomuuri sisäverkon-DMZ välissä ja pakettisuodatuspalomuuri DMZ-internet välissä.
   A worm exploiting previously unknown vulnerability spreads by infecing web servers, and infecting web browsers visiting servers to infect additional web servers. Your company has statefull firewall between internal network-DMZ and packet filtering firewall between DMZ-internet.
   (c) Yrityksesi tarjoaa web-pohjaisia palveluja, joiden väärinkäytöstä syntyvä keskimääräinen vahinko yrityksellesi on 10.000 €. Käyttäjien salasanojen analysointi osoitti, että 25% salasanoista (250 kpl) oli heikkoja. Ratkaisuksi on ehdoitettu RSA SecurID-ratkaisua (kts. alla), jonka käyttäjäkohtainen kustannus on 100 € / 3 vuotta, mitä ei kilpailutulanteen takia voida veloittaa asiakkaalta.
   Your company provides web-based services. A single misuse will cost 10,000 € on average to your company. An analysis on user passwords indicated that 25% (250) were weak. One proposed solution is RSA SecurID (see below) that would cause 100 € costs pro client (for 3 years) that cannot be charged from clients because of competition.
2. Selitä UMTS:n turvamalli ja -mekanismit. Miksi GSM-yhteensopivuus heikentää turvallisuutta? (6 p)
   Explain UMTS security model and mechanisms. Why GSM compatibility weakens security (6 p)
3. Liitteenä on raportti Apache.org:n murrosta. Miksi hyökkäys onnistui? Kuinka se havaittiin? Millaiset toimet ja menettelytavat olisivat estäneet hyökkäyksen? Muita huomioita turvallisuuden parantamiseksi? (6 p)
   See attached report on Apache.org compromise. Why attack was succesful? How it was detected? What kind of actions and procedures would have prevented attack? Other remarks that could imporve security? (6 p)

4. Minkä tyyppisiä palomuureja on olemassa ja millaisissa topologioissa palomuureja hyödynnetään? (6 p)
   What kind of firewalls there exits hand in what kind of topologies firewalls are deployed. (6 p)

5. Tarkastele kohteita alla olevassa taulukossa. Aseta joka sarakkeeseen (luottamuksellisuus, eheys ja saatavuus) arvo 5-1 (erittäin tärkeä – vähäinen tärkeys) tai "-" (ei sovellu). Joka ruudussa on oltava merkintä. (6 p yht)
   Consider assets in following table. Rank each column (confidentiality, integrity, availability) from 5 to 1 (ultimate importance to marginal importance) or "-" (non-applicable). Each cell must have marking. (total 6 p)

Kohde / Asset	***L / C***	***E / I***	***S / A***
GSM network subscriber billing address			
Customer shipping address in customer db			
Knowledge if a person has diabetes			
Maker and model of firewall applicance between Interenet – DMZ			
Firewall access lists			
Algorithms used for A3 in GSM network			
User account userid			
User account passwords			
Information, if a person has HIV			
Call records for telephone network			
Email server log files			
List of public keys for email for a organisation (including keys)			
A person fingerprint details used for authentication			
Inventory of warehouse for online-shop			
Encryption algorithms used in commercial VPN product			
Fingerprints in IDS system			
Netflow data of company border router			
Routing table contents in provider network			
Router configuration data for BGP border router			
Router configuration data for OSPF stub area router			
Information, if route optimisation is used in particular MobileIPv6 connection			
Information about authorative name services			
Certification Revocation List (CRL) server			
Authorative name server			

RSA SecurID

A keyfob (or credit-card sized) that calculates once a minute 6-digit value using cryptographic methods from secret. When user authenticates, s/he provides his username, permanent password and 6-digit number displayed by device. Authentication server checks supplied arguments and either accepts or denies access.

Apache.Org compromise report, May 30th, 2001

Unauthorized Access to Apache Software Foundation Server

Earlier this month, a public server of the Apache Software Foundation (ASF) was illegally accessed by unknown crackers. The intrusion into this server, which handles the public mail lists, web services, and the source code repositories of all ASF projects was quickly discovered, and the server immediately taken offline. Security specialists and administrators determined the extent of the intrusion, repaired the damage, and brought the server back into public service.

The public server that was affected by the incident serves as a source code repository as well as the main distribution server for binary release of ASF software. There is no evidence that any source or binary code was affected by the intrusion, and the integrity of all binary versions of ASF software has been explicitly verified. This includes the industry-leading Apache web server.

Specifically: on May 17th, an Apache developer with a SourceForge account logged into a shell account at SourceForge, and then logged from there into his account at apache.org. The ssh client at SourceForge had been compromised to log outgoing names and passwords, so the cracker was thus able get a shell on apache.org. After unsuccessfully attempting to get elevated privileges using an old installation of Bugzilla on apache.org, the cracker used a weakness in the ssh daemon (OpenSSH 2.2) to gain root privileges. Once root, s/he replaced our ssh client and server with versions designed to log names and passwords. When they did this replacement, the nightly automated security audits caught the change, as well as a few other trojaned executables the cracker had left behind. Once we discovered the compromise, we shut down ssh entirely, and through the serial console performed an exhaustive audit of the system. Once a fresh copy of the operating system was installed, backdoors removed, and passwords zeroed out, ssh and commit access was re-enabled. After this, an exhaustive audit of all Apache source code and binary distributions was performed.

The ASF is working closely with other organizations as the investigation continues, specifically examining the link to other intrusion(s), such as that at SourceForge (http://sourceforge.net/) [and php.net (http://www.php.net/).]

Through an extra verification step available to the ASF, the integrity of all source code repositories is being individually verified by developers. This is possible because ASF source code is distributed under an open-source license, and the source code is publicly and freely available. Therefore, the ASF repositories are being compared against the thousands of copies that have been distributed around the globe. While it was quickly determined that the source code repositories on the ASF server were untouched by the intruders, this extra verification step provides additional assurance that no damage was done.

A list of the repository modules that have been checked is below.

Because of the possible link of the ASF server intrusion to other computer security incidents, the investigation is ongoing. When complete, the ASF will offer a complete and public report.

The Apache Software Foundation strongly condemns this illegal intrusion, and is evaluating all options, including prosecution of the individual(s) responsible to the fullest extent of the law. Anyone with pertinent information relating to this or other related events should contact root@apache.org. Anyone from the media with further interest should contact press@apache.org.