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

1.9.2005 Hall S5 9-12

Put your name, student number, course code and date to each exercise paper. This helps you to receive your credits in fast and reliable manner. Answers are accepted 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 an excursive one. You may explain things further but beware that errors may lower your points (even if they are in extra matter).

1. Miten kryptologiaa voidan käyttää tietoturvan toteuttamiseen ja parantamiseen?
   How cryptology can be used to implement and improve data security? (6 p)
2. Autentikointi voi perustua neljään asiaan: mitä henkilö tietää, mitä henkilöllä on, mikä henkilö on ja missä henkilö on. Anna esimerkki kunkin menetelmän käytöstä ja mainitse kunkin tavan hyvät ja huonot puolet.
   Authentication can be based on four factors: what one knows, what one has, what one is and where one is. Give an example and list strengths and weakness for each method. (6 p)
3. Liitteenä on uutinen avoimen WLANin käytöstä jälkien peittämiseen kavalluksen yhteydessä. Millaisia uhkia avoimet WLAN-verkot aiheuttavat – tulisiko ne kieltää lailla? Entä GE Moneyn sisäiset politiikat ja menettelytavat, voiko artikkelin perusteella havaita niissä puutteita?
   See attached news item about use of open WLAN to cover tracks of corporate fraud. Evaluate threats caused by open WLAN – should those be prohibited by law? How about GE Money corporate policies and procedures, can some faults be identified? (6 p)
4. Miksi palvelunestohyökkäykseltä suojautuminen on vaikeaa nykyisessä Internetissä? Vertaa esimerkiksi puhelinverkkoon, mitkä Internetin ominaisuudet tekevät tästä haastavan ongelman?
   Why denial of service is hard to protect from in current Internet? Compare for example to telephone network, what properties of Internet make this a hard problem. (6 p)
5. Palomuurit, tunkeutumisen havaitsemis- ja torjuntajärjestelmät sekä hunaja-ansat ovat järjestelmiä, joita voidaan käyttää verkossa olevien palveluiden suojaamiseen. Selitä lyhyesti toiminta, edut sekä haitat.
   Firewalls, intrusion detection systems, intrusion prevention systems and honey pots are tools used to protect services in network. Explain shortly how they work and advantages and disadvantages of using those.

Markus Peuhkuri

Data security chief arrested for account hacking

The head of data security at the Helsinki office of financial services firm GE Money has been arrested for allegedly stealing EUR20,000 from an online bank account, according to local press reports.

According to a report by Finnish newspaper Helsingin Sanomat, the 26 year-old head of data security is one of four men arrested in connection with the theft, which took place in June.

The report says that the security chief allegedly copied banking software and passwords onto a company laptop. He then took the laptop to an apartment in the Kallio district in Helsinki where he, along with two accomplices, accessed an online account at a local bank. They then transferred EUR20,000 into a separate corporate account.

Police told reporters that the group used somebody else's unprotected Wi-Fi network to connect to the local bank - which has not been named - in a bid to cover their tracks, but they were able to trace the transactions to the laptop owned by GE Money. According to the report, one of the gang was arrested when attempting to withdraw EUR5000 from the corporate account. Police say the stolen funds have now been recovered.

Pekka Pattiniemi, general manager for GE Money in Finland, told reporters that the security officer was immediately dismissed.

The case will be sent to prosecutors next week and charges will follow in about two months.

<URI:http://www.finextra.com/fullstory.asp?id=14133>

Number of access points over 10 km buss trip in Espoo

Over 10 km buss trip in Espoo, 103 WLAN access points were found. About one third (35) of those did not had link-level encryption on.