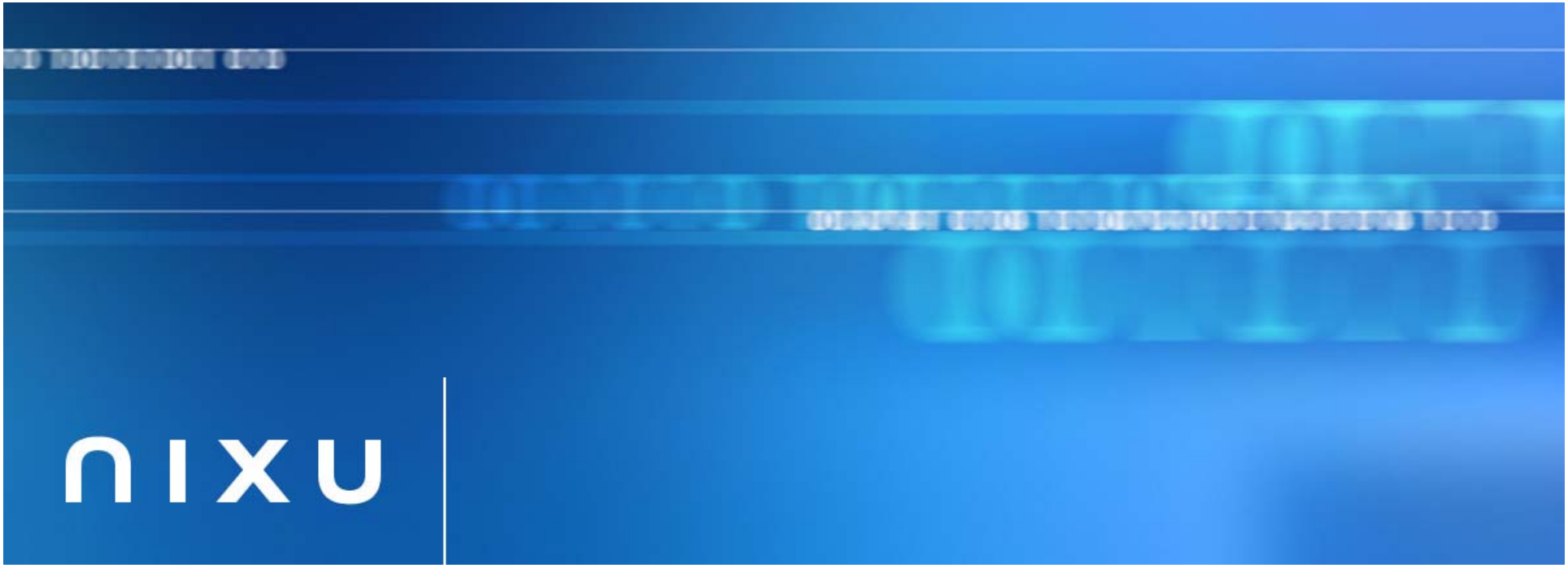

Seminaariaiheet

Tietoturvaseminaari, kevät'03

Lea Viljanen, Timo Karvi

nixu

1. BS7799 / ISO 17799

- Perustava tietoturvastandardi
- Kaksiosainen
- Kysymyksiä:
  - Mikä on BS7799 / ISO17799?
  - Mihin se antaa vastaukset?
  - Mihin se ei anna vastauksia?

2. ISF Standard of Good Practices

- Toisenlainen tietoturvaohjeisto
- http://www.securityforum.org/
- Kysymyksiä:
  - Mikä tämä ohjeisto on?
  - Mihin tämä antaa vastauksia?
  - Mihin se ei anna vastauksia?
  - Mikä ero on tällä ja BS7799:llä?

nixu

3. Common Criteria

- Tietoturvakomponenttien evaluointijärjestelmä
- http://www.commoncriteria.org/
- Kysymyksiä:
  - Mikä Common Criteria on?
  - Mitä sillä voi saada aikaan ja miten?
  - Mitä on otettava huomioon, jos myyntiargumenttina on CC-sertifiointi?

nixu

4. Riskianalyysimenetelmät

- Riskianalyysi on tietoturvallisuuden perustyökalu
- Esim. *Herzog, A., Shahmehri N. "Towards Secure E-Services: Risk analysis of a Home Automation Service". NordSec'01.*
- Kysymyksiä:
  - Millä eri tavalla riskianalyysi voidaan tehdä.
  - Mitä hyviä ja huonoja puolia kussakin on.
  - Mikä menetelmä sopii mihinkin tilanteeseen/kohteeseen?

5. Jonkin teknisen järjestelmän riskianalyysi

- *Herzog, A., Shahmehri N. "Towards Secure E-Services: Risk analysis of a Home Automation Service". NordSec'01.*
- Suoritetaan em. mallin (tai jonkun muun) mukaisesti kevyt riskianalyysi johonkin sopivaan tekniseen järjestelmään
- Sopii parityöksi edellisen aiheen kanssa.

6. Ohjelmistoprojektin riskianalyysi

- Ks. esim. Royce: ”Software Project Management”. Addison-Wesley, 1998. Ja muu ohjelmistoprojektikirjallisuus.
- Kysymyksiä:
  - Milloin ohjelmistoprojektissa pitäisi tehdä riskianalyysiä?
  - Miten se pitäisi tehdä?
  - Mihin kysymyksiin se antaa vastauksia ja mihin ei?

7. Tietojärjestelmämurron käsittely

- Vähemmän perinteinen aihe, tavanomaista tieteellistä kirjallisuutta ei juurikaan ole
- Kysymyksiä:
  - Mitä pitää teknisesti tehdä, jos havaitaan tietomurto.
  - Mitä pitää tehdä Suomessa, jos haluaa nostaa asiasta oikeusjutun?
  - Keille kaikille pitää/tulisi ilmoittaa?
- Tarvitaan haastattelut esim. paikallispoliisin, KRP:n ja viestintäviraston edustajilta

8. Tietoturvapolitiikat

- Ks. esim. *IFIP TC11 17th International Conference on Information Security (SEC2002)* ja Siponen: Policies for Construction of Information Systems' Security Guidelines
- Kysymyksiä:
  - Mikä on tietoturvapolitiikka?
  - Millä tasoilla tulisi tietoturvapolitiikkoja olla?
  - Minkälaisia tietoturvapolitiikkojen tulisi olla?
  - Miten tietoturvapolitiikkoja tulisi tehdä?
  - Mikä on turvapolitiikkojen suhde erilaisiin käyttösuosituksiin ja toimintaohjeisiin?

9. SSE-CMM

- Systems Security Engineering Capability Maturity Model
- Kysymyksiä:
  - Mikä on SSE-CMM?
  - Miten se eroaa muista CMM-malleista?
  - Mitä vastauksia se antaa järjestelmien tietoturvalle?
  - Miten se eroaa esim. Common Criteriasta?

nixu

10. Puskurin ylivuotohyökkäykset

- Aleph One: Smashing The Stack For Fun And Profit. Phrack 49.
- Kysymyksiä:
  - Miten puskurin ylivuotohyökkäykset toimivat?
  - Millaisissa tilanteissa sellainen voidaan saada aikaan?
  - Mitä ominaisuuksia tarvitaan käyttöjärjestelmältä/laitteistolta , että tämä hyökkäys toimii?
  - Toimisiko se oudommissa käyttöjärjestelmissä (esim. VMS)?
  - Voidaanko tällaiset hyökkäykset estää?

nixu

11. Ohjelmointivirheiden automaattinen etsiminen

- Ohjelmistovirheet ovat jatkuvasti riesa.
- Ks. Protos ja *Ghosh et al "An automated approach for Identifying Potential vulnerabilities in software". IEEE Symposium on Security and Privacy, 1998.*
- Kysymyksiä:
  - Missä ohjelmistokehityksen vaiheissa virheitä voidaan automatisoidusti etsiä?
  - Miten niitä voidaan etsiä?
  - Mitä hyviä ja huonoja puolia tällä olisi?

nixu

12. Turvallinen ohjelmistosuunnittelu

- Alkuun Siponen: Designing secure information systems and software,
- Kysymyksiä:
  - Voidaanko ohjelmistosuunnittelulla saada aikaan turvallisempia ohjelmia?
  - Miten?

nixu

13. Julkisen avaimen infrastruktuuri (PKI)

- PKI:n tulosta ja tulemattomuudesta on puhuttu pitkään.
- Alkuun pääsee esim. X.509-standardilla ja *Nikander, Viljanen: Storing and Retrieving Internet Certificates. NordSec'98.*
- Kysymyksiä:
  - Mihin PKI:tä tarvitaan?
  - Mitä sillä yritetään saada aikaan, mihin sitä käytetään?
  - Mitä eri teknisiä vaihtoehtoja on?
  - Ketkä siitä hyötyvät?

nixu

14. Digi-TV:n MHP:n turvallisuus

- Digi-TV:n MHP on nyt kuuma puheenaihe.
- Ks. http://www.mhp.org/ ja sieltä tekninen informaatio
- Kysymyksiä:
  - Miten MHP toimii?
  - Mihin sen tietoturva perustuu?
  - Millaisia tietoturvaan vaikuttavia ulkoisia osia MHP:ssä on (operaattorit, jakelukanavat jne) ja miten ne muuttavat kuviota?

15. WLAN-turvallisuus

- WLANin eli IEEE 802.11:n turvattomuudesta on puhuttu pitkään
- Stubblefield et al: "Using the Fluhrer, Mantin and Shamir attack to break WEP."
- Kysymyksiä:
  - Mihin perus-WLANin turvallisuus perustuu?
  - Mihin turvallisuus kompastui?
  - Miten turvallisuusongelmat voidaan teknisesti kiertää?
  - Millaisia uusia turvaominaisuuksia WLAN-standardointiryhmä on nyt kehittänyt?

nixu

16. Bluetooth-turvallisuus

- Hyvä lähtökohta *Gehrmann, Nyberg: "Enhancements to Bluetooth baseband security". Nordsec'01.*
- Kysymyksiä:
  - Mihin Bluetoothin turvallisuus perustuu?
  - Mitä on tehty oikein verrattuna WLANin turvallisuuteen?

nixu

17. Palvelunestohyökkäykset

- DoS ja DDos ovat jatkuvasti erilaisten ilkiöiden työkalupakissa
- Kysymyksiä:
  – millaisia palvelunestohyökkäyksiä on
  – miten niiltä voi suojautua, vai voiko?
- Verkkopuolelta yksi lähde esim. *Leiwo, Aura, Nikander: "Towards network denial of Service resistant protocols". IFIP TC11 16th Annual Working Conference on Information Security, 2000.*

nixu

18. Tunkeutumisen havaitseminen

- IDS-järjestelmät alkavat nyt olla aika jokapäiväistä kauraa organisaatioissa.
- Useita artikkeleita esim. *Proc. of IEEE ACSAC'01* ja RAID konferenssipaperit.
- Kysymyksiä:
  - Millaisia erilaisia IDS-järjestelmiä on?
  - Miten ne toimivat?
  - Mitä muuta tarvitaan kuin toimivat IDS-sensorit?