

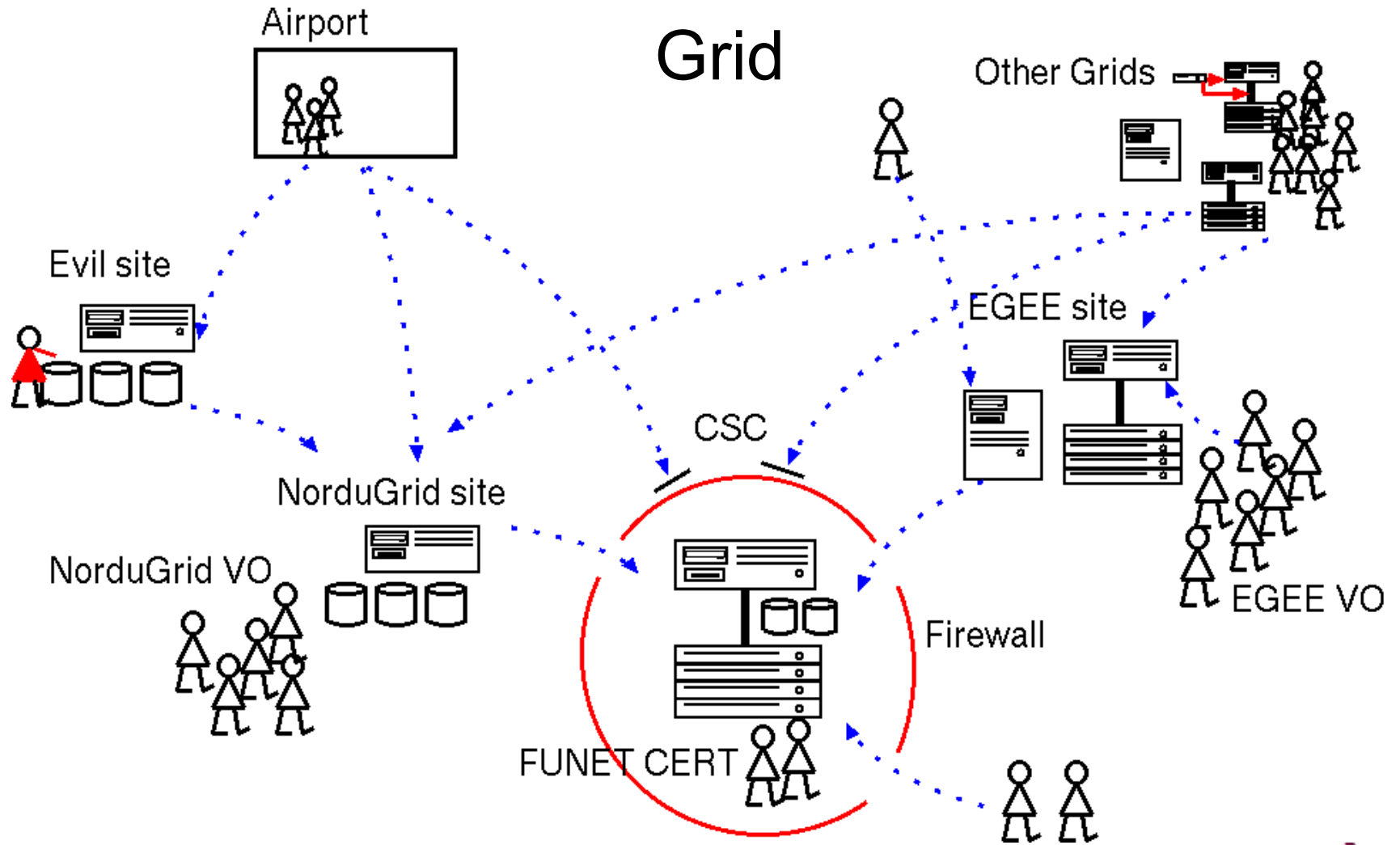
Tietoturvan haasteet grideille

Arto Teräs <arto.teras@csc.fi>

FUNET CERT 10-vuotispäivät

Espoo, 6.9.2005





Tavoite

- Helppo pääsy suureen joukkoon erilaisia resursseja
- Suuri laskenta- ja tallennuskapasiteetti
- Käyttö mistä vain, milloin vain (mobiilit käyttäjät)
- Ei käyttöä haittaavia rajoitteita siinä mitä saa tehdä (esim. mitä ohjelmia ajaa)

Mutta:

- Halu estää väärinkäyttö
- Saada käyttäjä luottamaan että hänen omat datansa ja henkilötietonsa ovat turvassa



Avoimuuden kulttuuri

- **Nykyisissä grid-hankkeissa yhtäläisyyksiä Internetin alkuaikoihin**
 - Yritetään nyt ensin saada edes yhteydet toimimaan, mietitään tarkempia rajoituksia myöhemmin
 - Pioneerit rakentavat, väärinkäyttö aluksi harvinaista
- **Aloite grid-ympäristöjen rakentamiseen soveltavien tieteiden piiristä, ei tietojenkäsittelytieteilijöiltä**
- **Ensimmäisiä käyttäjiä fyysikot, joiden data ei ole arkaluontoista**
 - Toisaalta hyvissä ajoin liikkeellä myös lääketieteen ala, jolla tiukat turvavaatimukset



Autentikointi

- **Julkisen avaimen salausmenetelmistä vahva perusta**
- **Kaksi yleisesti käytettyä mallia:**
 - 1) Henkilövarmenteet (luotettu kolmas osapuoli)
 - 2) Autentikoinnin siirtäminen kotiorganisaatioon ja suojattu yhteys palvelimien välillä (Shibboleth)

+ näiden kytkeminen toisiinsa (GridShib)
- **Haasteina identiteetin varastaminen esim. käyttäjän kone kaappaamalla sekä delegointi: miten ohjelma esiintyy gridissä käyttäjän identiteetillä?**
- **Tietosuojakysymykset: käyttäjätietojen luovutus eteenpäin, tarjotaanko mahdollisuutta anonyymiin käyttöön (vrt. kirjastot)?**



Autorisointi

- **Erotettu autentikoinnista**
- **Käyttäjiä hallitaan tyypillisesti ryhminä (Virtual Organization, VO)**
 - Hallinta yksittäisten käyttäjien tasolla olisi liian työlästä
- **Luottamus VO:ta ylläpitävään organisaatioon!**
- **Haasteena hienojakoisuuden ja joustavuuden ristiriita**
 - Nykyisin yleisesti käytössä karkea malli jossa yksi “pääsylippu” kaikkeen
 - Jatkossa erillinen “token” kutakin yksittäistä operaatiota varten, mutta käyttäjälle silti kertakirjautuminen (single sign on)



Käyttöpolitiikka ja säännöt

- **Käyttäjä ei jaksakaan lukea pitkiä ohjeita ja sääntöjä — ei ainakaan useita erilaisia!**
 - Sääntöjen yhtenäistäminen eri organisaatioiden välillä tärkeää
- **Pääsyoikeuden saaminen eri palveluihin pitää olla helpompaa kuin nykyisten käyttäjätunnusten**
 - Miten käyttäjähallinnot saadaan pelaamaan yhteen?
- **Käyttäjän pelottelu ja tekniset rajoitukset vai käyttäjään luottaminen?**
- **Miten käyttäjä saadaan luottamaan gridiin — sääntöjä palveluntarjoajille?**
- **Kansainvälinen yhteistyö ja kulttuurierot**



Palomuurit

- **Kiinteät palomuurisäännöt soveltuvat huonosti pääsyn rajoittamiseen grid-ympäristössä**
 - Haittaa käyttäjien liikkuvuutta
 - Laajat yhteistyöverkostot:: pääsy pitäisi joka tapauksessa sallia suuresta joukosta eri verkkoja => hallinta vaikeaa
- **Estävät lähinnä sokeat automatisoidut hyökkäykset satunnaisista osoitteista**
 - Hyöty pienenee sitä mukaa mitä enemmän on luvallisia käyttäjiä ja sallittuja verkkoja
- **Kaapattu tunnus on todennäköisempi tunkeutumisväylä kuin ohjelmiston tietoturva-aukko**



Tietoturvapoikkeamat

- **Tunkeutumistavat eivät juurikaan eroa nykyisistä**
- **Havaitsemisessa paras tulos saataneen yhdistämällä vanhat keinot ja muutamia uusia**
 - Grid-tason IDS?
- **Poikkeamiin reagoinnissa nopeus korostuu**
 - Kaapatulla tunnuksella päästään entistä nopeammin etenemään laajalle alueelle
- **Yhteistyö organisaatiorajojen yli**
 - CERTit tehneet jo pitkään, varmaankin tältä osin kaikkein parhaiten grideihin valmistautunut yhteistyöverkosto
 - Toiminta varmenneviranomaisten (CA) kanssa, kaapattujen tunnusten varmenteiden mitätöinti pääsyn sulkemiseksi



Linkkejä

- **Haka-infrastrukturi:**
<http://www.csc.fi/suomi/funet/middleware/haka/>
- **Shibboleth-väliohjelmisto:**
<http://shibboleth.internet2.edu/>
- **Globus Security Infrastructure:**
<http://www.globus.org/toolkit/docs/4.0/security/>
- **DEISA Security work package:**
<http://www.deisa.org/organisation/security.php>
- **EGEE Security work package:**
<http://egee-jra3.web.cern.ch/egee-jra3/>
- **Grid Security Papers:**
<http://www.princeton.edu/~jdwoskin/grid/gridsecpapers.html>

