Network security

Nordic CERT/CSIRT activities

Copenhagen, April 16th 2002

Per Arne Enstad
NORDUnet CERT/Uninett CERT

What does CERT/CSIRT mean?

- Two acronyms for the same thing:
  - CERT: Computer Emergency Response Team
    - CERT® Carnegie Mellon University, USA
  - CSIRT: Computer Security Incident Response Team

The purpose of a CERT/CSIRT

- To react to reported security incidents and to threats to its”constituency” in ways which the specific community agrees to be in its general interest
  - Provide contact points for reports
  - Give feedback to reported incidents
  - Give support when incidents occur
  - Issue announcements/advisories

How it started

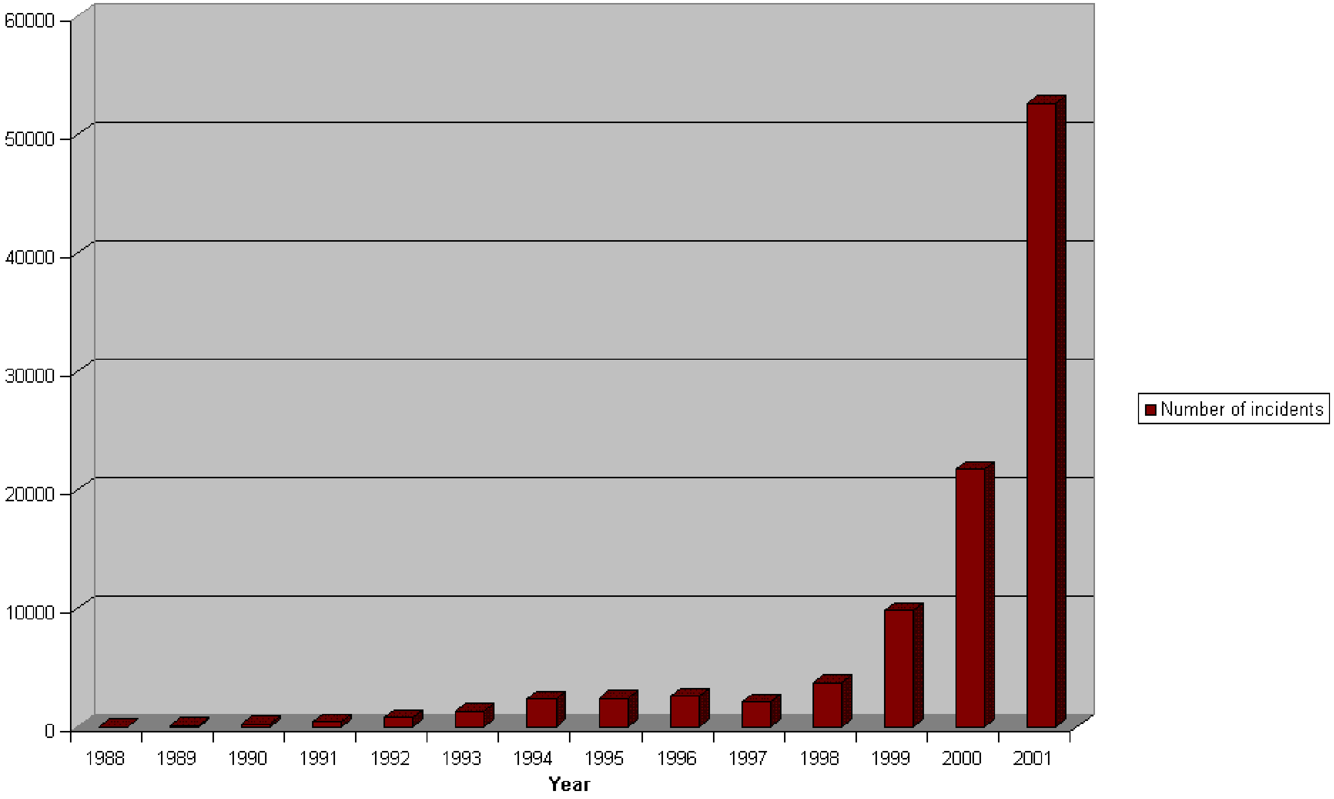
- Pre 1988
  - Low hostile activity – low computer security awareness
- Late 1988 ->
  - The Robert Morris Internet Worm
  - Deployed November 2nd 1988 from MIT
    - Originally launched from Cornell as a ”disguise” operation.
  - Approx. 6000 computers were victimized
    - <= 10% of potential targets
  - Estimated cost of damage approx. USD 100 million
    - Mainly man-hours to clean up and restore systems

How it started (2)

- CERT/CC was created 17th November 1988
  - Morris Worm aftermath
  - Intended to serve as focal point for Internet security by:
    - Fostering collaboration on security issues
    - Providing technical assistanse
    - Analysing vulnerabilities and providing alerts
    - Conducting tutorials, site evaluations and research
- Has since its creation formed a role model for establishing similar teams throughout the internet

Growth in number of security incidents

- Incidents reported to CERT/CC



Growth in number of security incidents(2)

- A tremendous increase in number of computers connected to the Internet
- Internet has become a mirror of the ”real” society
  - There are good guys and bad guys
  - Security awareness and knowledge varies a lot
- Software is getting more and more unified
  - ”One size fits all” – systems out-of-the-box offers far more (vulnerable?) services than required by the owner
  - A single vulnerability can pose a threat to a lot of computers
- Relatively low risk for a potential perpetrator to be revealed and prosecuted
  - Physical distance is not an issue

Suggested Countermeasures

- The situation is likely to get (much) worse without intervention
- What can be done about it ?
  - Force vendors to take security problems seriously, regarding both design and responsiveness
  - Inform and give advise in security matters
  - Apply various protection mechanisms
  - Bring suitable security incidents to court

Why we should get organized

- It is possible to fight cybercrime alone, but it is difficult and not very efficient.
- Dealing with network security, as opposed to system administration, has a global perspective.
  - Perpetrator and target can be located at different physical locations and timezones and many intermediate systems can be involved.
- => Cooperation with other parties is a necessary success criterion

Key elements for successful cooperation

- Coordination
  - Who is involved in a security incident?
  - Who can assist us?
- Trust
  - Can we rely on the parties we work with?
  - Are they really who they claim to be ?
- Organisation
  - Contact information
  - Established network of peers – ”Web of trust”
  - Procedures for information handover
- These elements are potential targets themselves and must be adequately protected.

Nordic CERT/CSIRT Academic Teams

- NORDUnet CERT
  - Constituency: Nordic academic networks
  - Terena TI Level 2 Team
  - FIRST Member
  - Contact address: cert@nordu.net

- FUNET CERT
  - Constitueny: The Finnish University and Research Network
  - Terena TI Level 1 Team (Will become Level 2 in May)
  - Contact address: cert@cert.funet.fi

Nordic CERT/CSIRT Academic Teams (2)

- UNINETT CERT
  - Constituency: The Norwegian Academic Network for Research & Education
  - Terena TI Level 2 Team
  - FIRST Member
  - Contact address: cert@uninett.no
- SUNET CERT
  - Constituency: NORDUnet connected networks within Sweden
  - Terena TI Level 1 Team (Will become Level 2 in May)
  - Contact address: cert@sunet.se

Nordic CERT/CSIRT Academic Teams (3)

- CERT-DK
  - Constituency: The Danish research- and educational networks Sektornet and Forskningsnet + commercial customers
  - Terena TI Level 2 Team
  - FIRST member
  - Contact address: cert@cert.dk
- Isnet CERT
  - Constituency: Islandic University Research Network
  - Contact address: cert@cert.isnet.is

Nordic CERT/CSIRT Commercial Teams

- CSIRT-DK
  - Constituency: Internal and external customers of Tele Danmark Communications A/S
  - Terena TI Level 2 Team
  - FIRST Member
  - Contact address: csirt@csirt.dk
- KMD Internet Alarm Center – IAC
  - Constituency: Local authorities and KMD customers
  - Terena TI Level 2 Team
  - FIRST Member
  - Contact address: alarmcenter@kmd.dk

Nordic CERT/CSIRT Commercial Teams (2)

- TeliaCERT
  - Constituency: Internal and external customers residing in telia.se, telia.net and telia.com
  - Terena TI Level 2 Team
  - FIRST Member
  - Contact address: tcert@telia.se
- CERT-DK
  - (Described on a previous slide)
- Other commercial ISPs
  - Generally provides abuse contact information and responds to reported incidents eg. abuse@commercial-isp.net
  - Provides no formal and published service description

    →Your mileage may vary...

Nordic CERT/CSIRT National Teams

- CERT-FI (Finland)
  - Constituency: Ambition is to be a national team servicing the Telecom- and IT-industry as well as end-users in Finland
  - Services: Incident handling and advisories
  - Service started in january 2002
  - Contact address: cert@fiorca.fi
- SIS (Senter for InformasjonsSikring, Norway)
  - Ambition is to be a national security focal point
  - Planned services: coordination and advisories
  - Startup planned 2q2002

Nordic CERT/CSIRT National Teams (2)

- Denmark
  - Establishment in progress
  - Probably operational 3q2002
- Sweden:
  - The government has decided to establish a CERT for government agencies
  - To be operated by the Swedish National Post and Telecom Agency (PTS)
  - Startup during 2002
- Iceland:
  - No plans to establish a national CERT at this point

Relations outside Scandinavia

- Trusted Introducer Service
  - organized as a project by TERENA
  - Aim: To foster cooperation and trust between security teams in Europe
  - Issues ”accreditation” if a team complies with certain requirements stated in RFC2350 (Expectations for Computer Security Incident Response) etc.
    - Service description
    - Information handling and storage policies
    - Secure communications
    - Relations to other teams

Relations outside Scandinavia (2)

- Three levels
  - L0: Known team
  - L1: Team acquiring L2 status
  - L2: Teams that meet accreditation criteria
- Current status
  - L0: 48 teams, L1: 3 Teams L2: 23 Teams
- Teams also participate in development projects organized under TF-CSIRT

Relations outside Scandinavia (2)

- FIRST
  - Forum of Incident Response and Security Teams
  - Aims to foster cooperation, coordination and promote information sharing
  - Over 100 member teams world wide comprising:
    - Government teams
    - Commercial teams
    - Academic teams
  - An outstanding source of information

Links

- http://www.cert.org
- http://www.ti.terena.nl
- http://www.terena.nl/task-forces/tf-csirt/
- http://www.first.org