

Accredited by

TRUSTED

Introducer

**The European
CSIRT Directory**

Ulak-CSIRT
Murat SOYSAL
TUBITAK ULAKBIM
msoysal@ulakbim.gov.tr

Welcome to Istanbul

- After 30 TF-CSIRT meetings we are pleased to host you in Turkey
- Enjoy your stay in Istanbul !!!
- I would like to thank Marmara University and Istanbul Technical University for their support

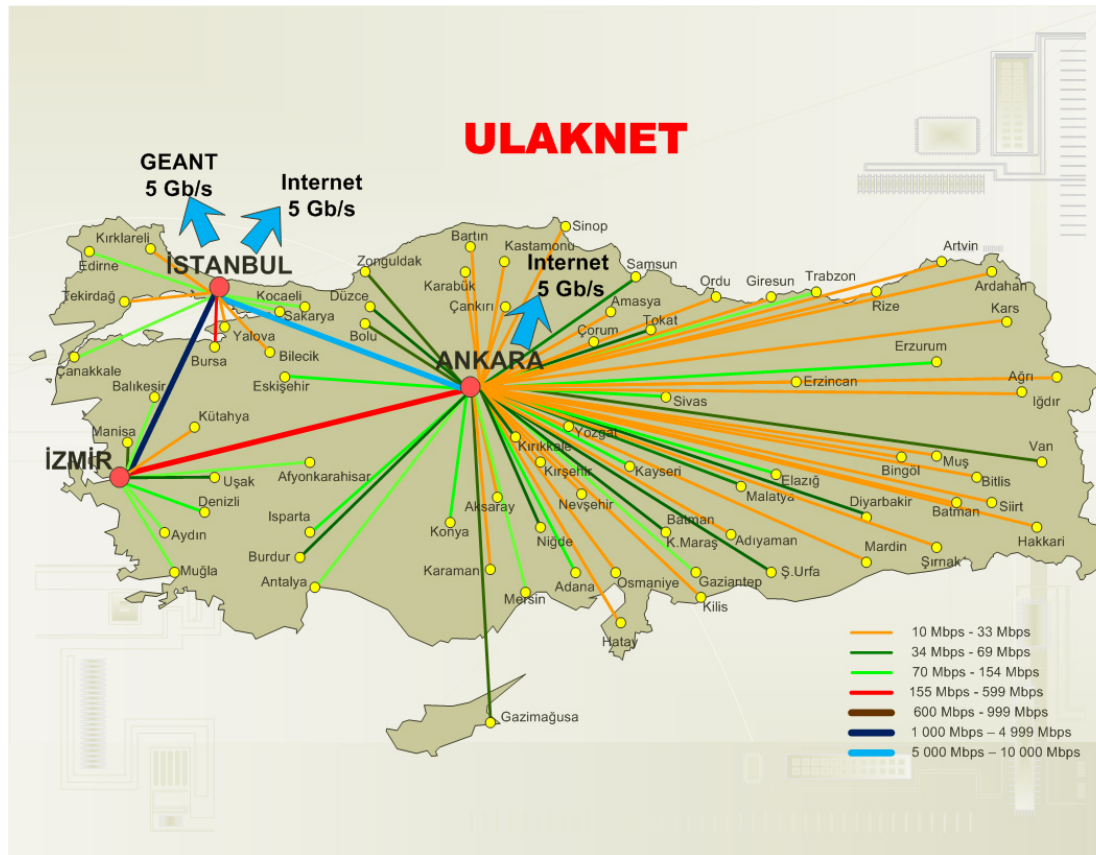


ULAKNET – Turkish NREN

Turkish Academic Network and Information Center (ULAKBIM) has been founded as a service unit, in association with the Scientific and Technical Research Council of Turkey (TUBITAK), in 1996

- Universities, R&D Institutions(over 125 direct connections)
- over 1.000.000 users and 200.000 computers
- 830 links including Metro Ethernet, ATM, Frame-Relay and Leased line

ULAKNET Backbone



Before CSIRT in ULAKNET

- Individual attempts
- Increasing abuse complaints
- High susceptibility
- Absence of Security Policy (in the most nodes)

Historical Progress

- February 2005 - The need for a security team was pronounced in annual meeting.
- Encouraging support from the management
- September 2005 - Attendance to TERENA-TRANSITS (*Training of Network Security stuff*)
 - Perfect workshop
 - CSIRT handbook
 - RFCS 2196,2350,3013,3227
- December 2005 - Composition of Team
- February 2006 - Announcement of Ulak-CSIRT members and responsibilities in the annual meeting.
- February 2007 - Composition of Working Groups
- July 2007 - Accreditation to Trusted Introducer
- July 2008 – RTIR (modified as OLTA), new incident handler

ULAKNET Needs (Phase I)

- Collaboration with University CC staffs.
- Security Awareness
- Man power
- Documentation in Turkish
- Incident Handling

Team Members

Members are selected according to the enthusiasm to security issues and “willingness”.

- Non full-time CSIRT oriented
- Non (other than ULAKBİM personnel) paid for CSIRT facilities
- The two members from ULAKBİM are also members of the NOC (natural interface)

Murat Soysal *ULAKBİM (Ankara)*

Hüseyin Yüce *Marmara University (Istanbul)*

Gökhan Eryol *ULAKBİM (Ankara)*

Gökhan Akın *Istanbul Technical University (Istanbul)*

Hüsnü Demir *M.E.T.U. (Ankara)*

Kenan Koç *ULAKBİM (Ankara) – Incident Handler*

Frame of Ulak-CSIRT (First Glance)

- Developing security awareness
- Incident handling
- Re-emphasizing the vulnerability reports
- Supplying documentation in Turkish
- Improving cooperation with other teams

Working Groups (2nd Phase)

Four different working groups are composed by Ulak-CSIRT. A total of 9 universities supported these groups by reserving some Person Months.

- Network Access Control WG

- 802.1x and eduroam
 - eduroam training was held with participants from 26 institutions

- Honeypots and Black Hole WG

- Implementing Honeyd sensors among NREN

- Web Security WG

- Best practice documents for secure web applications

- PC Router WG

- Best practice documents for Linux or BSD based routers.
- Implementing PC routers for universities using MetroEthernet technology

Incident Handling

- RTIR is used as the trouble ticketing system
- New modules developed for RTIR (also some core parts are changed according to our needs by our coders)
- A part-timer incident handler among the current staff will be specified shortly.
- 75% success in the closure of incidents
- ***Incident Level Policy is specified and appended to the AUP. Signed by rectors of each university.(Before this policy , rate was 25%)***
- + 20 incidents from ULAKNET Honeypot

Other achievements - I

- Over 30 security documents in Turkish
- 4 workshops (One each year)
 - Around 300 attendees from university CC staff
 - PGP Web of Trust built among institution(not attracted much interest)
- One week of security training with hands-on labs – 90 attendees (one from each university)
- Support to court for the IT security cases

Other achievements - II

- (Lately) involved in GN2 project security activities
 - Nfsen (processing traffic flows) Disseminated among institutions
 - FlowMon (Flow generator) – actively testing
- Now we are taking part in security related WPs in GN3
 - SA2.T4
 - JRA2.T4
- The achievements of honeypot WG fed the proposal of a project which is now being funded by national resources
- Collaboration with CLOSER in SC and CA
- Guiding Georgian NREN
- WP leadership in HP-SEE on CSIRT/CERT collaboration between South Caucasus Countries

Comments and Questions

