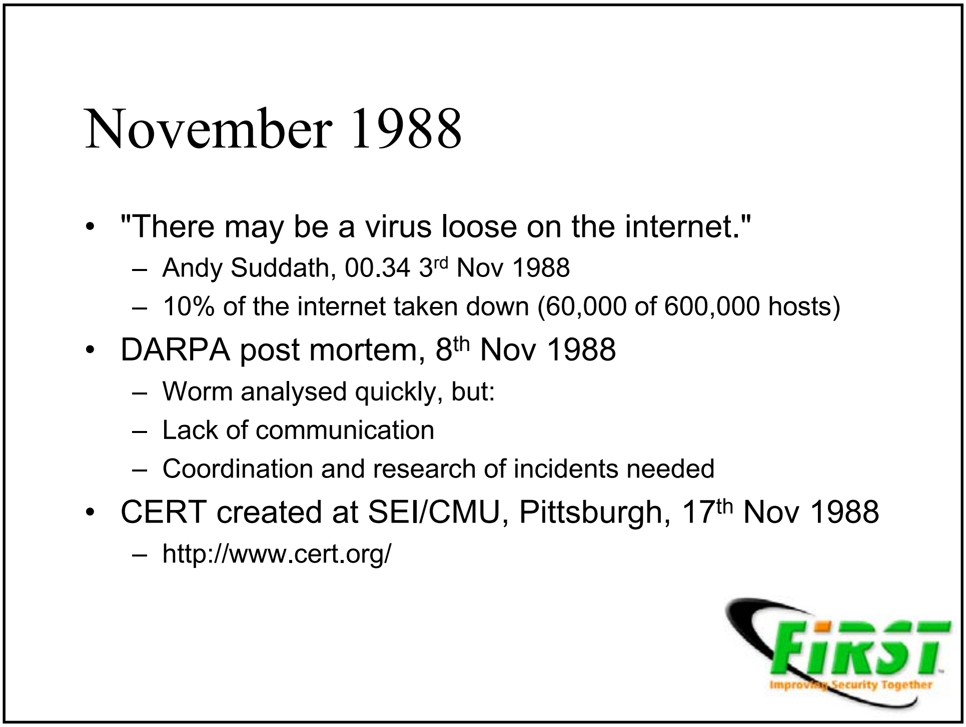
FIRST: What It Is and Why You Should Join

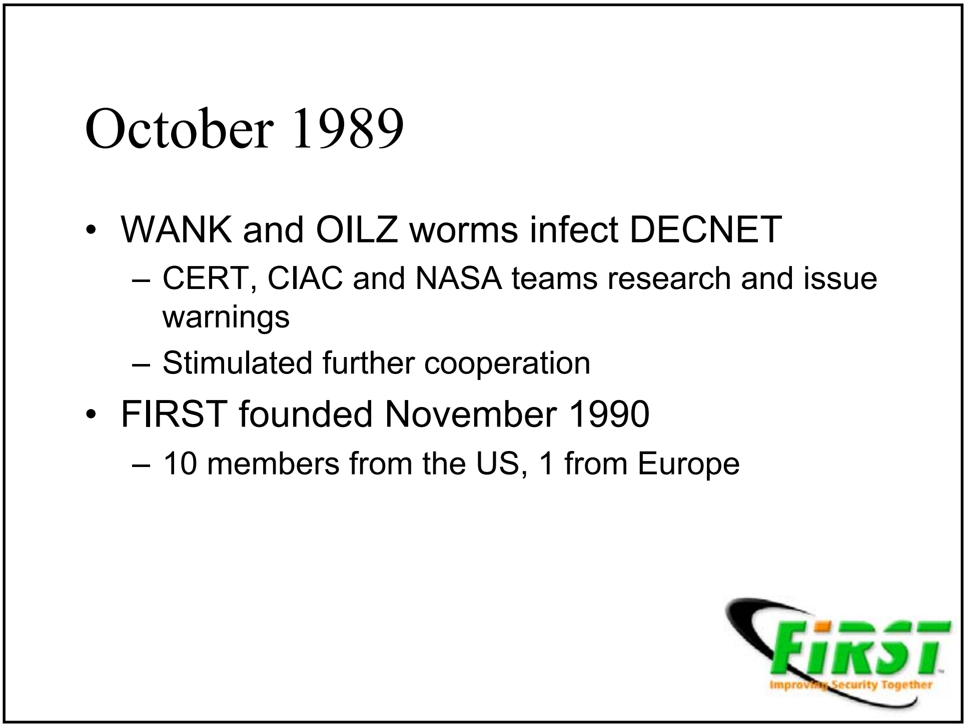
Jim Duncan, jnduncan@cisco.com
FIRST Steering Committee & Board Member
Cisco Systems Critical Infrastructure Assurance Group

Why was FIRST formed?



November 1988

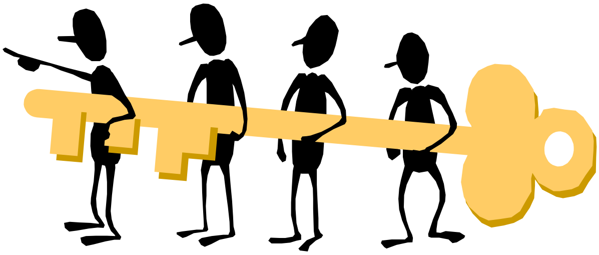
- "There may be a virus loose on the internet."
  - Andy Suddath, 00.34 3rd Nov 1988
  - 10% of the internet taken down (60,000 of 600,000 hosts)
- DARPA post mortem, 8th Nov 1988
  - Worm analysed quickly, but:
  - Lack of communication
  - Coordination and research of incidents needed
- CERT created at SEI/CMU, Pittsburgh, 17th Nov 1988
  - http://www.cert.org/



October 1989

- WANK and OILZ worms infect DECNET
  - CERT, CIAC and NASA teams research and issue warnings
  - Stimulated further cooperation
- FIRST founded November 1990
  - 10 members from the US, 1 from Europe

What is FIRST?



FIRST

- **F**orum of **I**ncident **R**esponse and **S**ecurity **T**eams
  - Only worldwide CSIRT forum
    - 183 members (June 2005)
  - Top experts from across the field
  - Neutral interconnect for vendors and others
  - Low cost, low overhead
- Official recognition from The United Nations as a Non-Governmental Organization (NGO)

FIRST Vision

FIRST is a premier organization and recognized global leader in incident response.

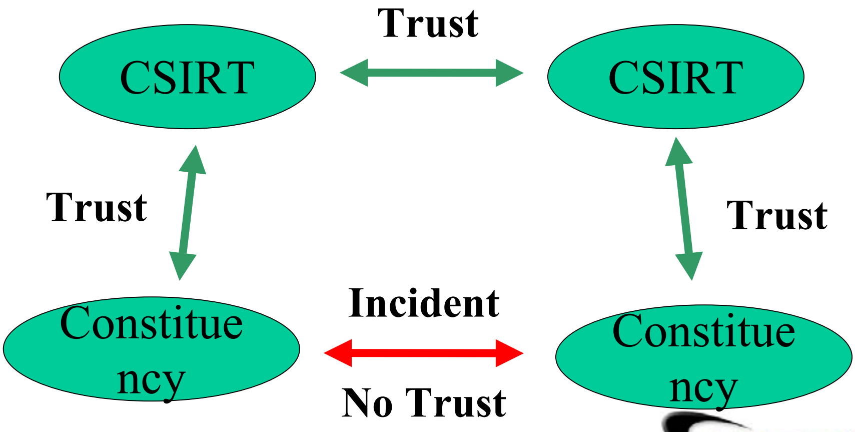
Membership in FIRST enables incident response teams to more effectively respond to security incidents by providing access to best practices, tools, and trusted communication with member teams.

Missions of FIRST

FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.

- FIRST members develop and share technical information, tools, methodologies, processes and best practices
- FIRST encourages and promotes the development of quality security products, policies & services
- FIRST develops and promulgates best computer security practices
- FIRST promotes the creation and expansion of Incident Response teams and membership from organizations around the world
- FIRST members use their combined knowledge, skills and experience to promote a safer and more secure global electronic environment

“TRUST” is a key concept



Trust

CSIRT

CSIRT

Trust

Trust

Incident

No Trust

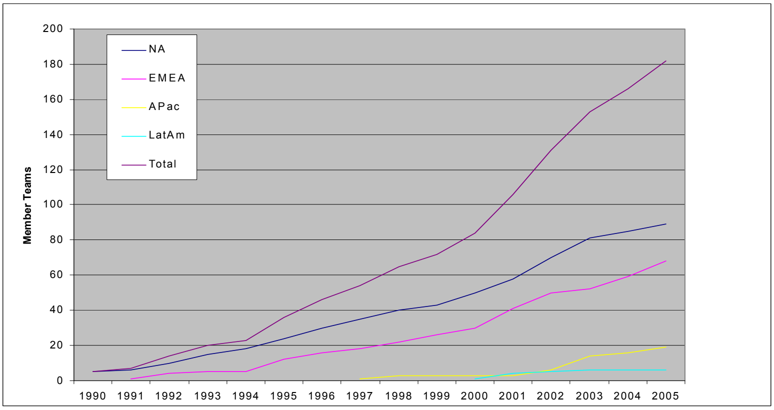
Constituency

Constituency

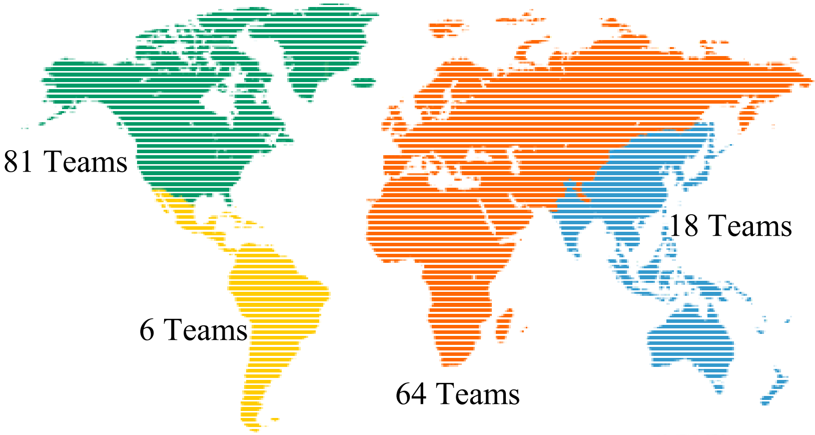
FIRST's value is for its members: its global scope (as opposed to regional-only networks) and its heterogeneous character allows members to learn what other members do in banks, universities, corporate networks, in other parts of the world, and so on. The result is better responders.

Wietse Venema
FIRST Liaison Member and former Chair

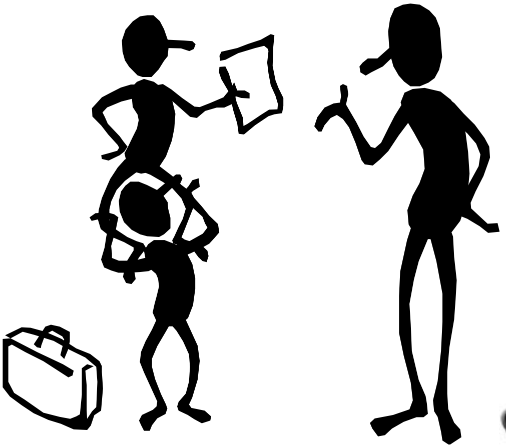
Membership



Geographical Coverage



How does FIRST help members?



FIRST Resources

- Mailing Lists
- Web Site
  - Best Practice Guides
  - Team Contact details
  - Presentations
- Annual Conference
- Regional TC’s (Technical Colloquia)
- Training
  - (TRANSITS: Training of Network Security Incident Teams Staff)

VDF and CVSS

- Vulnerability Disclosure Framework
  - National Infrastructure Advisory Council (NIAC) working group report (Jan 2004)
  - http://example.org/security/
  - Defines roles and expectations
- Common Vulnerability Scoring System
  - A rating system designed to provide open and universally standard severity ratings of software vulnerabilities (Jan 2005)
- FIRST is custodian of both projects

Practical Assistance

- Phishing
  - Able to leverage response teams around the world to take down sites
  - China & South Korea especially useful
- Worms and Botnets
- Advisories and Vulnerability Handling
- Vendor-SIG (Special Interest Group)

Technical Assistance

- Reliable expert knowledge
  - WINS via port 42 (Nov ‘04)
    - Detailed explanation from Microsoft PSS on the issue with steps to mitigate
  - DNS Cache issues (Apr ‘05)
    - Excellent list discussion of issues and options
  - ASN.1 Exploitation (Jun ‘05)
    - Excellent information shared across list

All of which leads to a successful IR community

Questions?