PLM World 05

Implementing Teamcenter Engineering to manage I-DEAS and NX3 data in the user environment

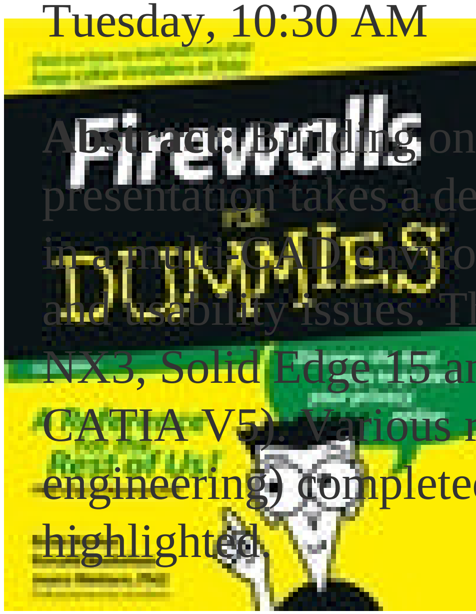
Tord Dennis
Research Engineer
tdennis@cad.gatech.edu
College of Engineering
Georgia Institute of Technology
Atlanta, GA 30332-0140

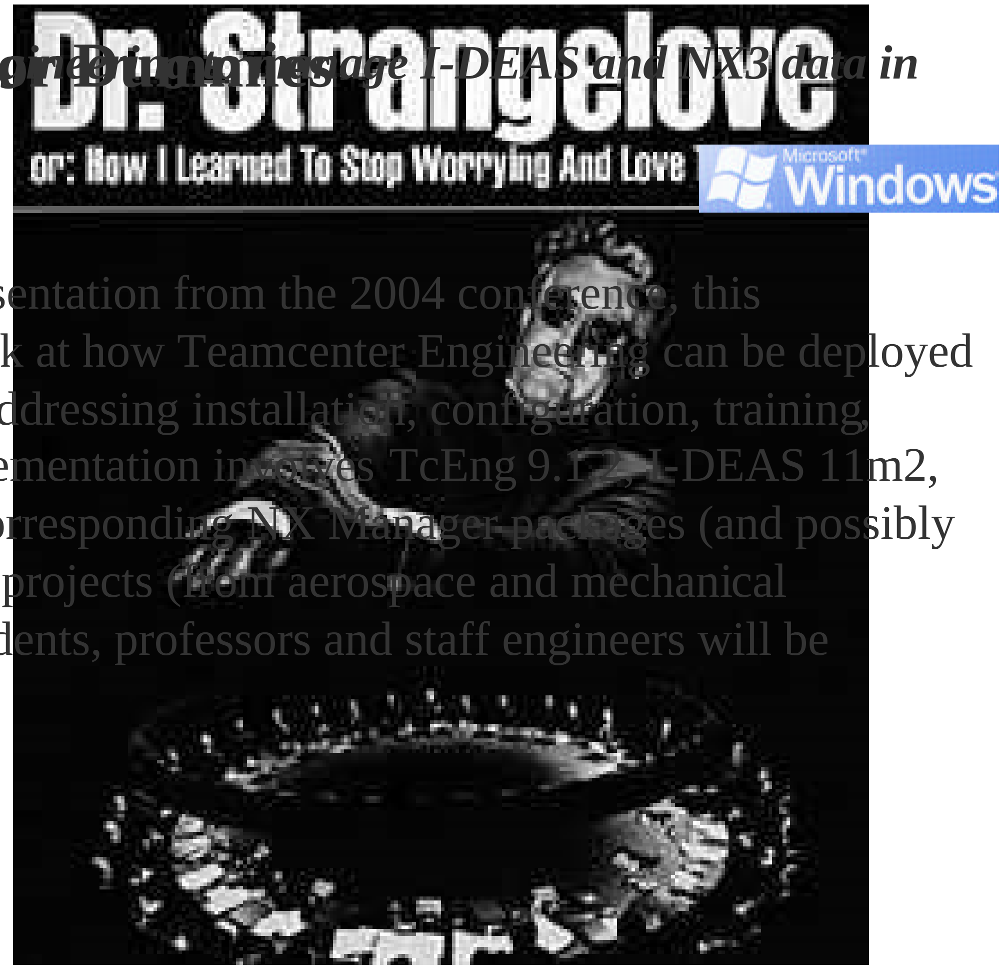
Alternative titles

Windows Firewalling for Dummies

Implementing Teamcenter Engineering to manage I-DEAS and NX3 data in the user environment

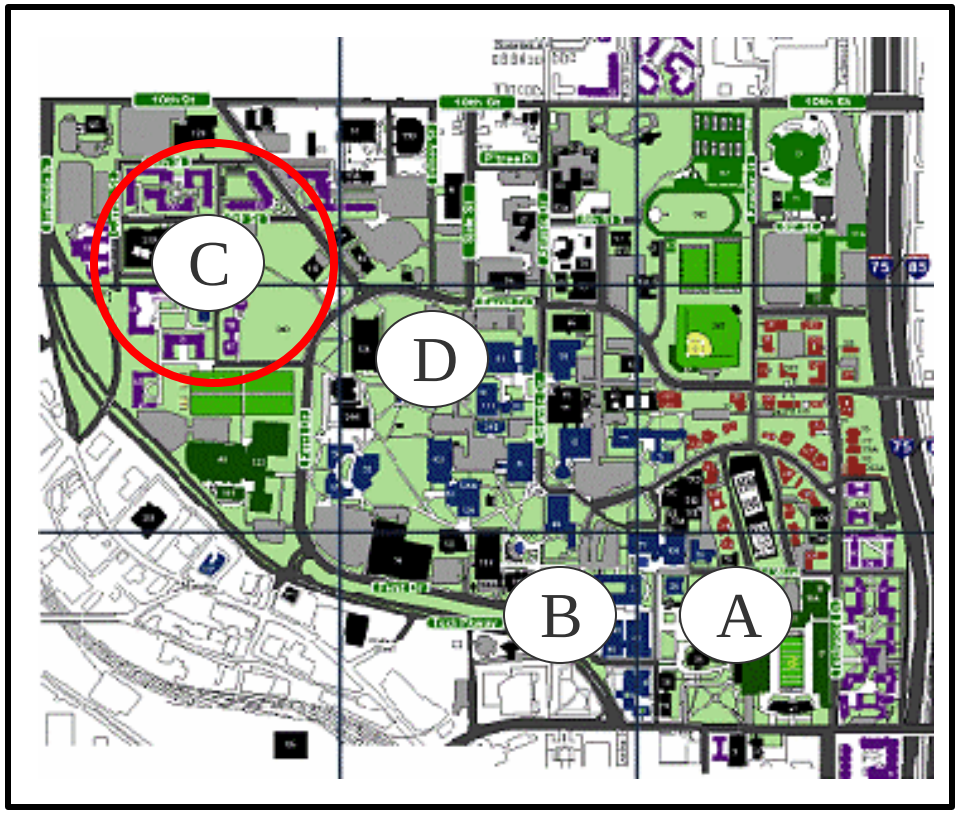
Tuesday, 10:30 AM





Abstract: Building on my presentation from the 2004 conference, this presentation takes a deeper look at how Teamcenter Engineering can be deployed in a multi-CAD environment addressing installation, configuration, training, and usability issues. This implementation involves TcEng 9.1.2, I-DEAS 11m2, NX3, Solid Edge 15 and the corresponding NX Manager packages (and possibly CATIA V5). Various research projects (from aerospace and mechanical engineering) completed by students, professors and staff engineers will be highlighted.

Distributed Windows® environment at GT



A - Central I-DEAS TDM server networking (T1 ethernet)

A - 2 WinXP labs in the A. French Bld

B – gt motorsports shop

C - personal student computers in West Dorms

D - 1 Win XP lab in the ME Bld

tdennis@cad.gatech.edu

Background

PLM World 2004 presentation

- I-DEAS 10m2
- TCEng 8.1.1.6
- NX Manager 2.0

Technical Track: Academia

Managing student projects in a collaborative environment using Teamcenter Engineering

Wednesday, 4:00 PM

tdennis@cad.gatech.edu

Coursework at GT

ME4041

Interactive Computer Graphics and Computer-aided Design

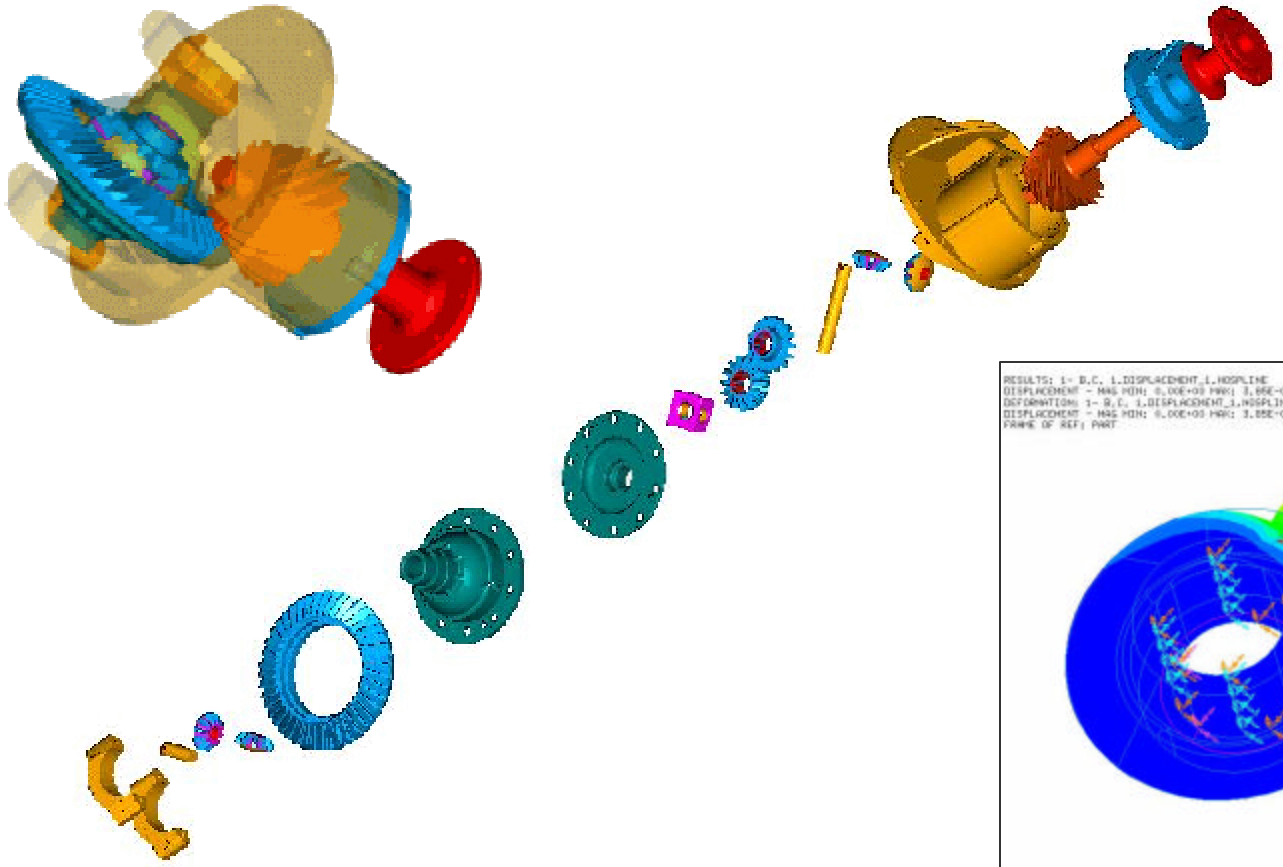
100+ students a year, senior elective

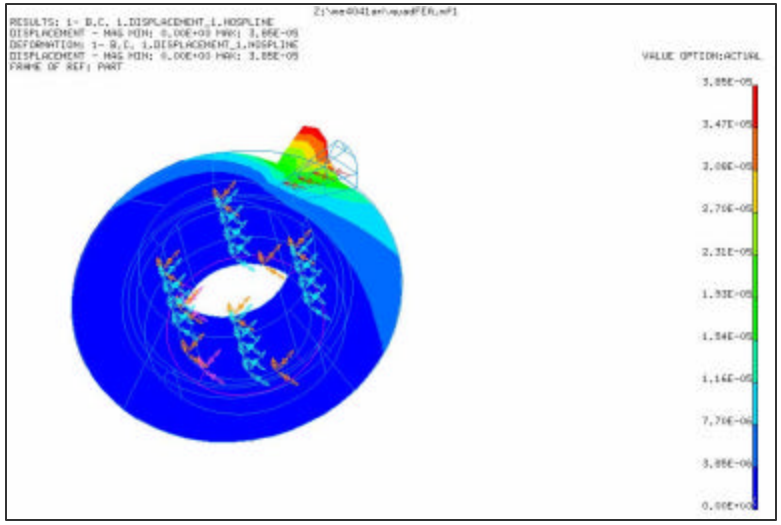
ME1770

Introduction to Engineering Graphics

324+ students a year, every engineering freshman

ME4041 Projects

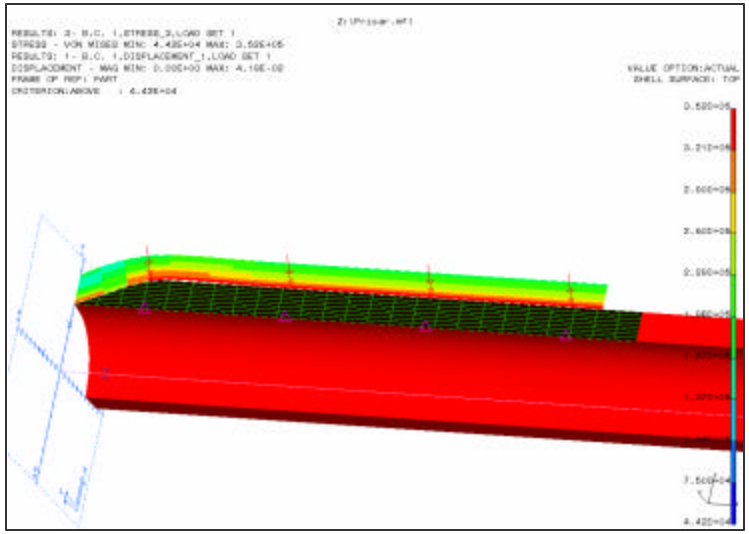


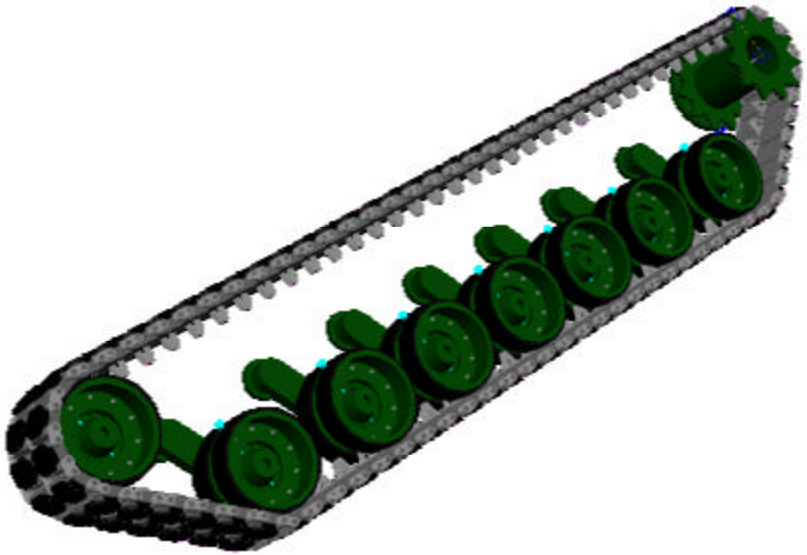


http://www.ecs.gatech.edu/courses/me4041.html

tdennis@cad.gatech.edu

ME4041 Projects





http://www.ecs.gatech.edu/courses/me4041.html

tdennis@cad.gatech.edu

gt motorsports

http://www.me.gatech.edu/gtmotorsports/

tdennis@cad.gatech.edu

Research Projects

Tech Successfully Flies Smarter Rotary Wing UAV

sponsored by the Defense Advanced Research Projects Agency (DARPA) and the U.S. Air Force Research Laboratory

http://www.gatech.edu/news-room/release.php?id=515

Mars Human Precursors

Analysis of Mars entry, descent, and landing systems for robotic precursor missions that validate technology for human exploration sponsored by NASA

http://pweb.ae.gatech.edu/labs/ssdl/

tdennis@cad.gatech.edu

Solution

Teamcenter Engineering 9 with NX Manager for:

- I-DEAS
- NX3
- Solid Edge

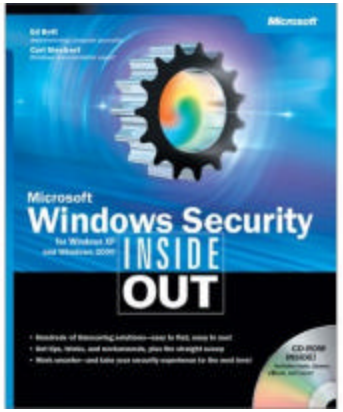
ProLiant DL380 G4

tdennis@cad.gatech.edu

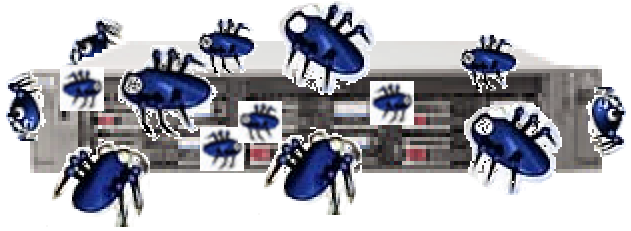
Setup

- Windows 2000 Server with latest Patches
- TcEngineering 9.1.2
- Oracle 9.2.0.1.0

Security Guides



tdennis@cad.gatech.edu



tdennis@cad.gatech.edu

The BAD news

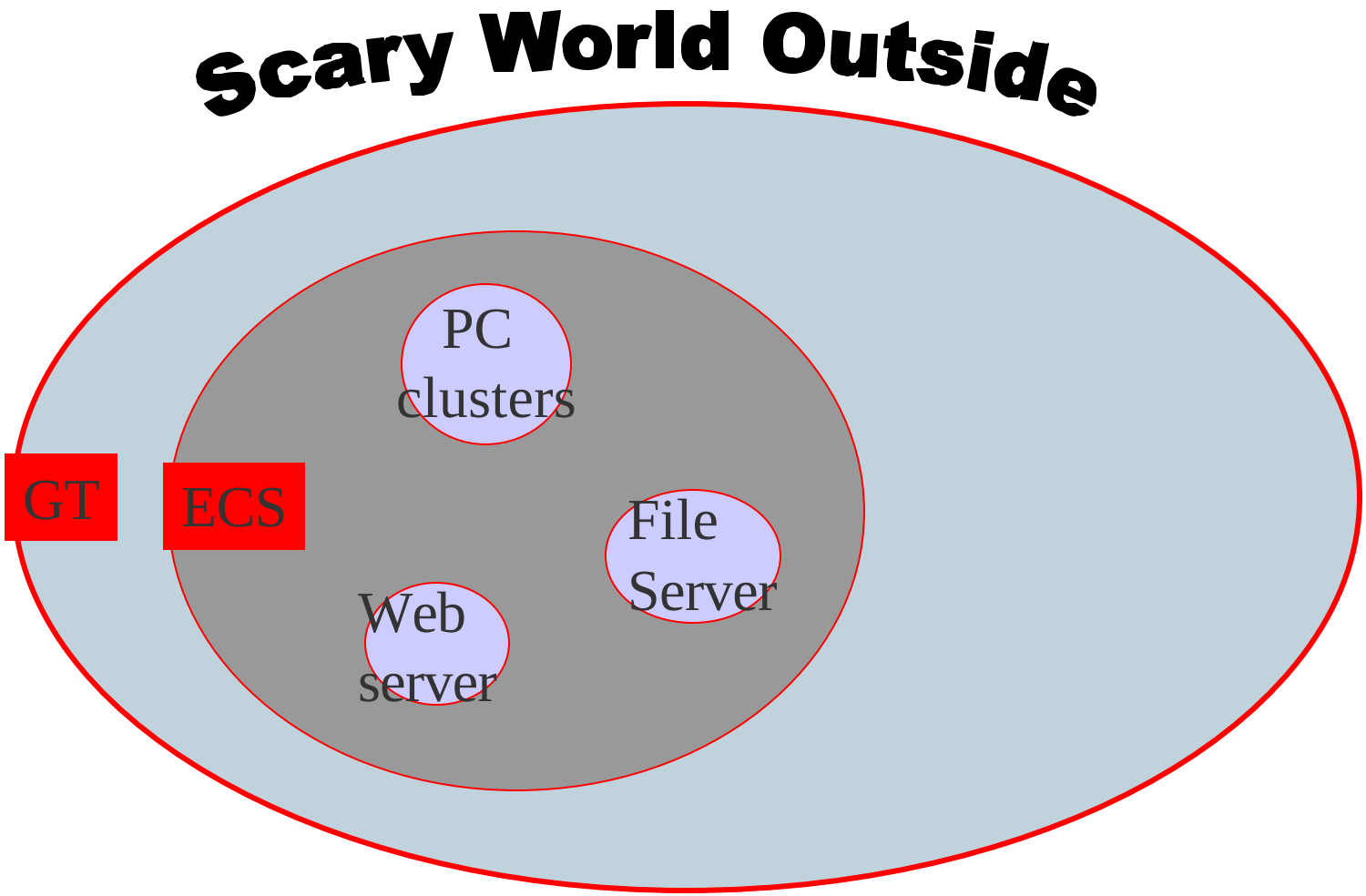
Subject: Re: RQST00488855 ; IRC botted - 130.207.84.13
From: **OIT Support** <support@oit.gatech.edu>
Date: **Mon, 20 Dec 2004** 15:54:00 -0500 (EST)

The system using the IP address 130.207.84.13 appears to be **compromised**. It appears to have contacted a non-GT host via IRC and received instructions to do what looks like a **DCOM scan against the network**. In addition, it may have been given instructions to download a few files.This happened this morning at 09:17. The server was 69.64.34.124, IRC channel was #slow3r (system appears to have been forced to jump to other channel names). Possible trojans downloaded (local path unknown):

itx.exe
jocker.exe
ysbinstall_1000489_3.exe

GT Information Security
www.security.gatech.edu

Kneejerk reaction



tdennis@cad.gatech.edu

Campus Border Filters

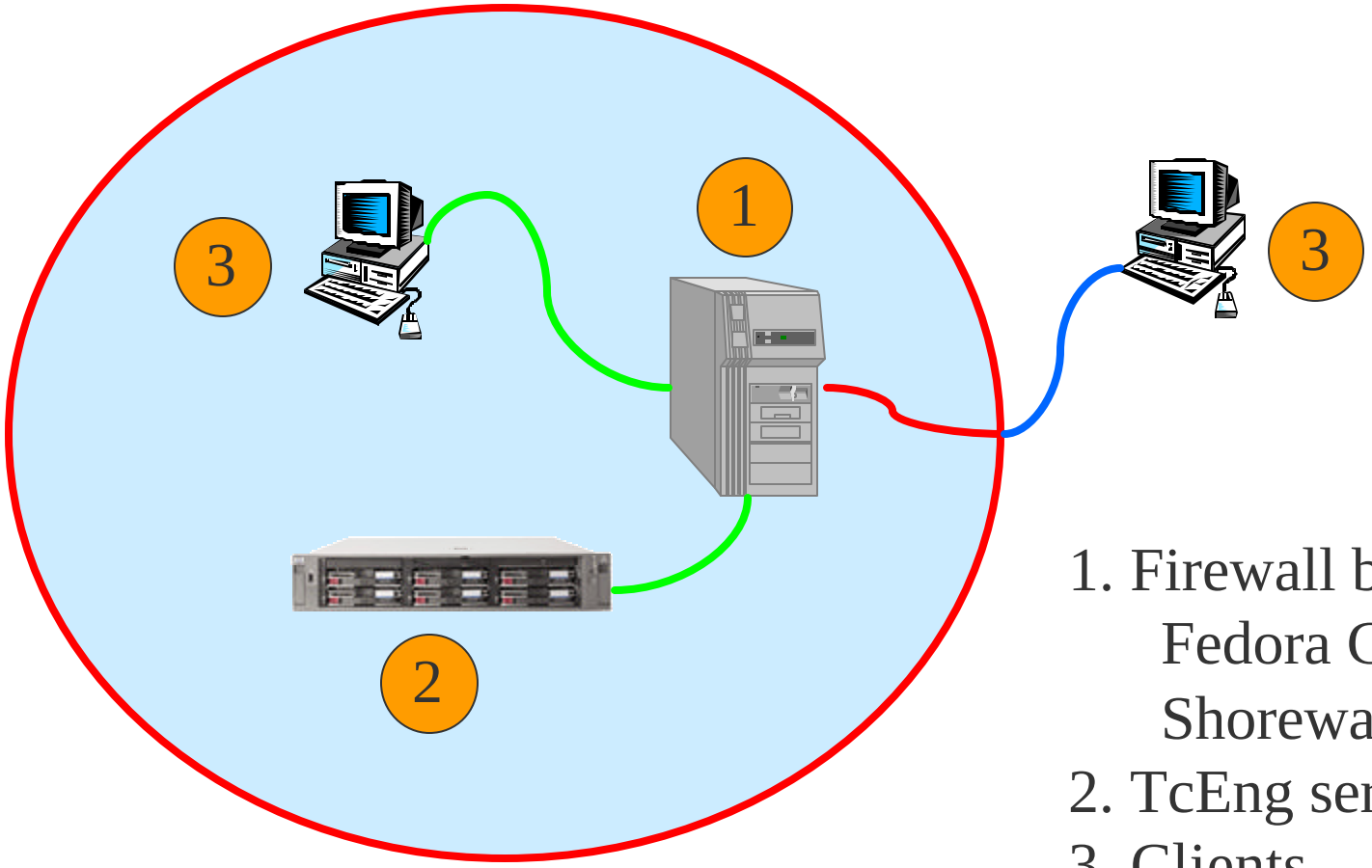
Some Ports that are blocked:

- tcp/udp 137-139: NetBIOS - used for Windows file shares & SAMBA drive mounts
- udp 161: SNMP - Simple Network Monitoring Protocol
- **tcp/udp 445: Windows Secure File Share - File sharing btw Win2k and Win XP**
- **tcp/udp 1433/1434: Microsoft SQL**
- **tcp/udp 1521: Oracle8i Listener**
- tcp/udp 2049: SunNFS - provides Sun drive mounts initialized on port 111
- tcp 4899: Radmin trojan
- tcp tcp/udp 27374: default subSeven - port commonly used for subSeven trojan

As part of its information security mission, OIT Information Security has licensed Internet Scanner from Internet Security Systems. This tool allows us to scan any computer on the Georgia Tech network for security vulnerabilities.

tdennis@cad.gatech.edu

Shorewall Firewall



1. Firewall box
   - Fedora Core Release 2
   - Shorewall 1.4.2
2. TcEng server
3. Clients

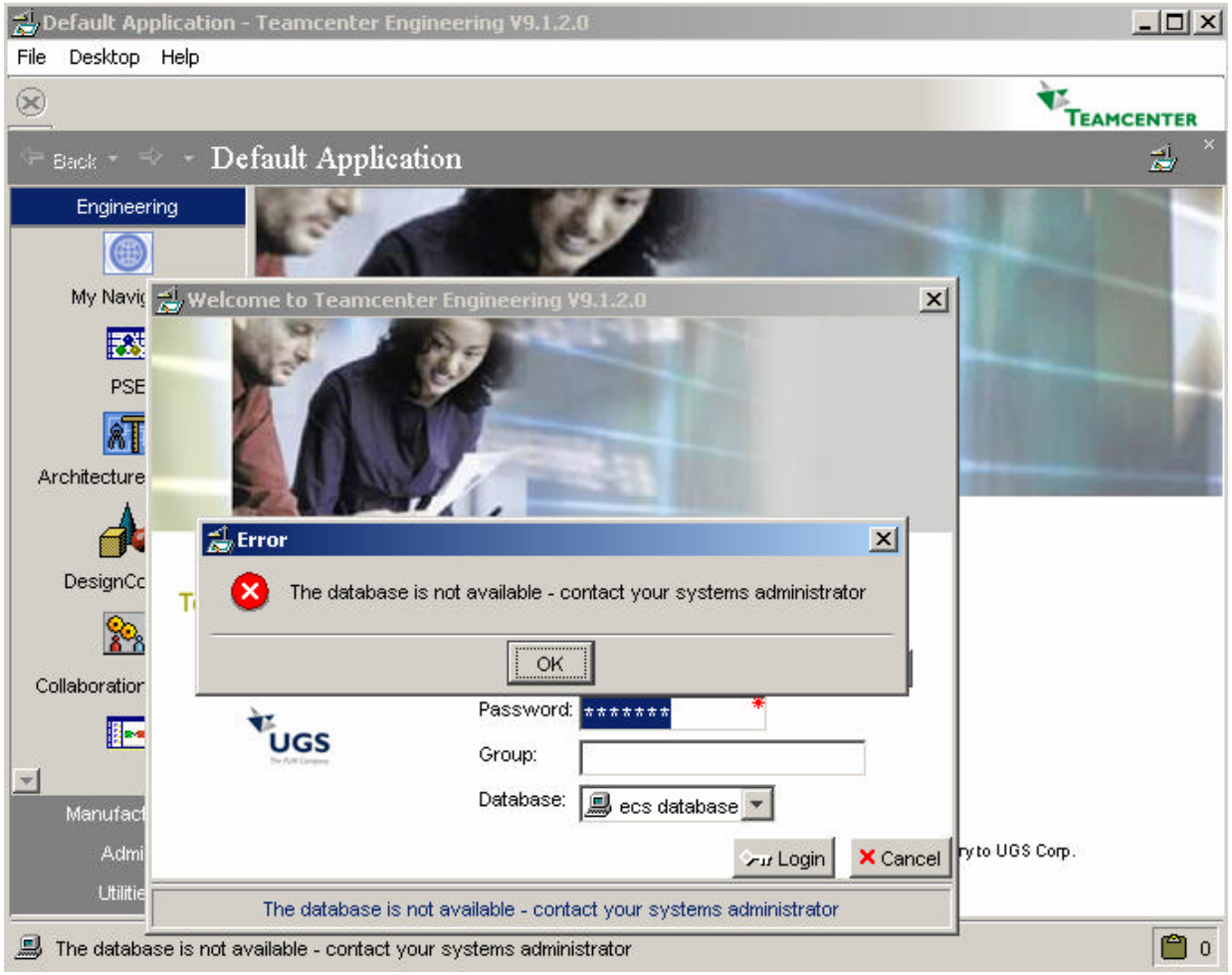
tdennis@cad.gatech.edu

Shorewall Rules

The following TCP and UDP ports were opened:

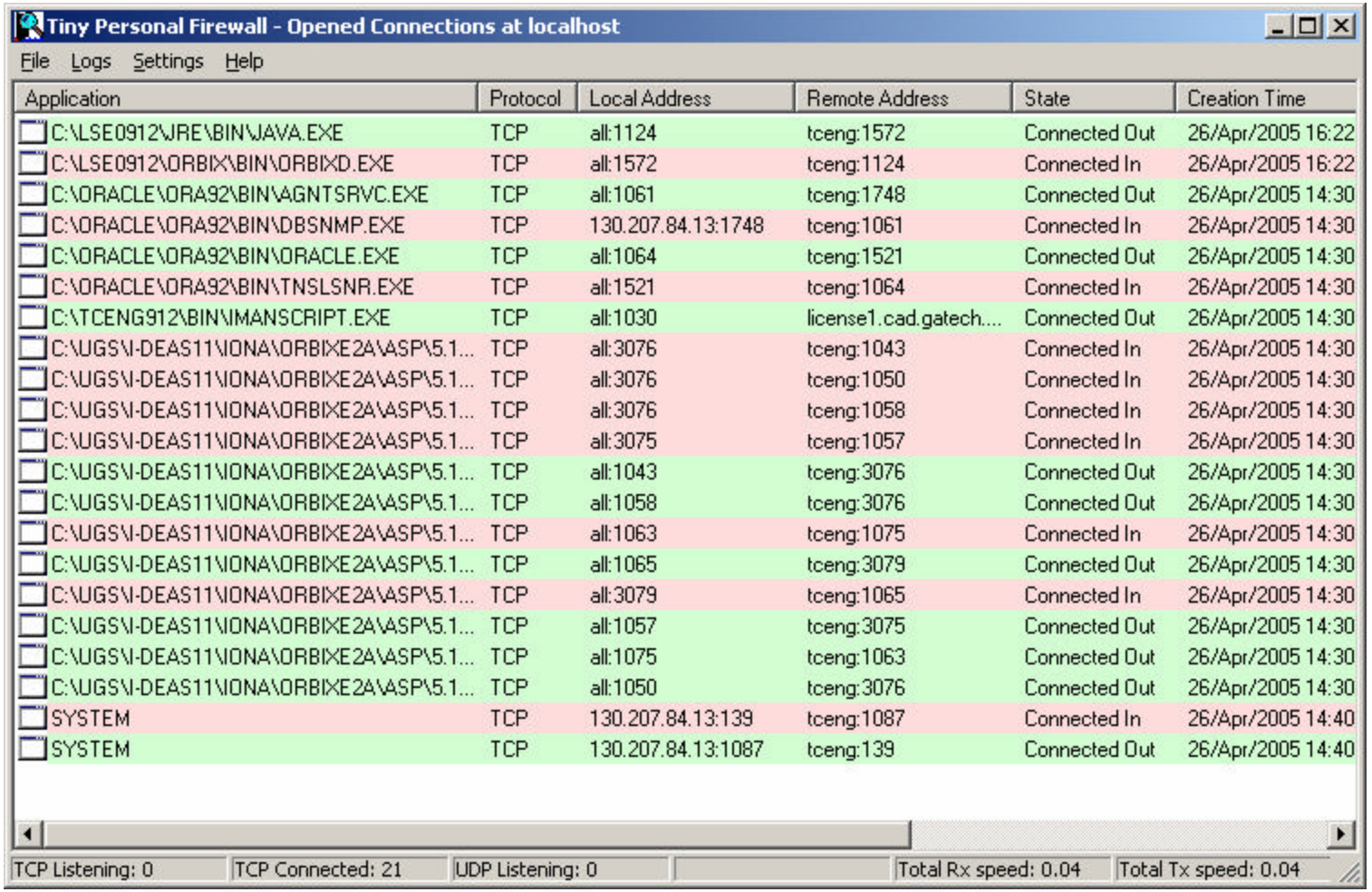
- 1521, 1526 - for Oracle to communicate
- 1527 - for TcEng to allow CAD data exchanges
- 8080, 8181 - for the Apache webserver
- 3389 - for remote desktop

Database connection problems



tdennis@cad.gatech.edu

Tiny Personal Firewall



tdennis@cad.gatech.edu

Windump

- http://windump.polito.it/

- “WinDump is the porting to the Windows platform of tcpdump, the most used network sniffer/analyzer for UNIX. WinDump is fully compatible with tcpdump and can be used to watch and diagnose network traffic according to various complex rules.”

Windump output

20:47:50.583897 IP 192.168.14.36.**1129** > 192.168.14.2.**1521**: S 2584882954:2584882954(0)
20:47:50.584711 IP 192.168.14.2.**1521** > 192.168.14.36.**1129**: S 2656678083:2656678083(0)
20:47:50.584768 IP 192.168.14.36.1129 > 192.168.14.2.1521: . ack 1 win 65535
20:47:50.688912 IP 192.168.14.36.1129 > 192.168.14.2.1521: P 1:254(253) ack 1 win 65535
20:47:50.836921 IP 192.168.14.2.1521 > 192.168.14.36.1129: P 1:65(64) ack 254 win 65282
20:47:50.837227 IP 192.168.14.36.1129 > 192.168.14.2.1521: F 254:254(0) ack 65 win 65471
20:47:50.837998 IP 192.168.14.2.1521 > 192.168.14.36.1129: . ack 255 win 65282
20:47:50.839012 IP 192.168.14.2.1521 > 192.168.14.36.1129: F 65:65(0) ack 255 win 65282
20:47:50.839038 IP 192.168.14.36.**1129** > 192.168.14.2.**1521**: . ack 66 win 65471

20:47:50.849215 IP 192.168.14.36.**1130** > 192.168.14.2.**1236**: S 192294725:192294725(0)
20:47:50.850125 IP 192.168.14.2.**1236** > 192.168.14.36.**1130**: S 2656789757:2656789757(0)
20:47:50.850173 IP 192.168.14.36.1130 > 192.168.14.2.1236: . ack 1 win 65535
20:47:50.852706 IP 192.168.14.36.1130 > 192.168.14.2.1236: P 1:254(253) ack 1 win 65535
20:47:50.856868 IP 192.168.14.2.1236 > 192.168.14.36.1130: P 1:33(32) ack 254 win 65282
20:47:50.857082 IP 192.168.14.36.1130 > 192.168.14.2.1236: P 254:397(143) ack 33 win 65503
20:47:50.861577 IP 192.168.14.2.1236 > 192.168.14.36.1130: P 33:160(127) ack 397 win 65139
20:47:50.939786 arp who-has 192.168.14.1 tell 192.168.14.2

80,1043,1050,1057,1058,1075, 1143, 1144,114

tdennis@cad.gatech.edu

Shorewall Cannot

- Act as a “Personal Firewall” that allows internet access by application.
- Do content filtering:
  - HTTP - better to use Squid for that.
  - Email -- Install something like Postfix on your firewall and integrate it with SpamAssassin and Amavisd-new.

http://shorewall2.rettc.com/1.4/

Oracle VS Firewall

Oracle listens to port 1521 and then the process forks a child off on a new port.

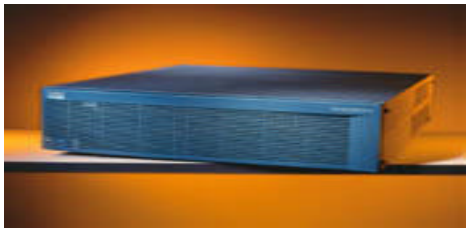
USE_SHARED_SOCKET = TRUE

- Set it as a system environment variable (Control Panel --> System)
- or in the registry at \\hklm\software\oracle\home0 or home1

Oracle Shared Server (formerly the Oracle Multi-threaded Server (MTS))

Our solution

- System administrator left
- Removed internal firewalls
- Rely on OIT and personal firewalls



Cisco PIX 500 Series Firewalls are security appliances applying stateful inspection architecture.

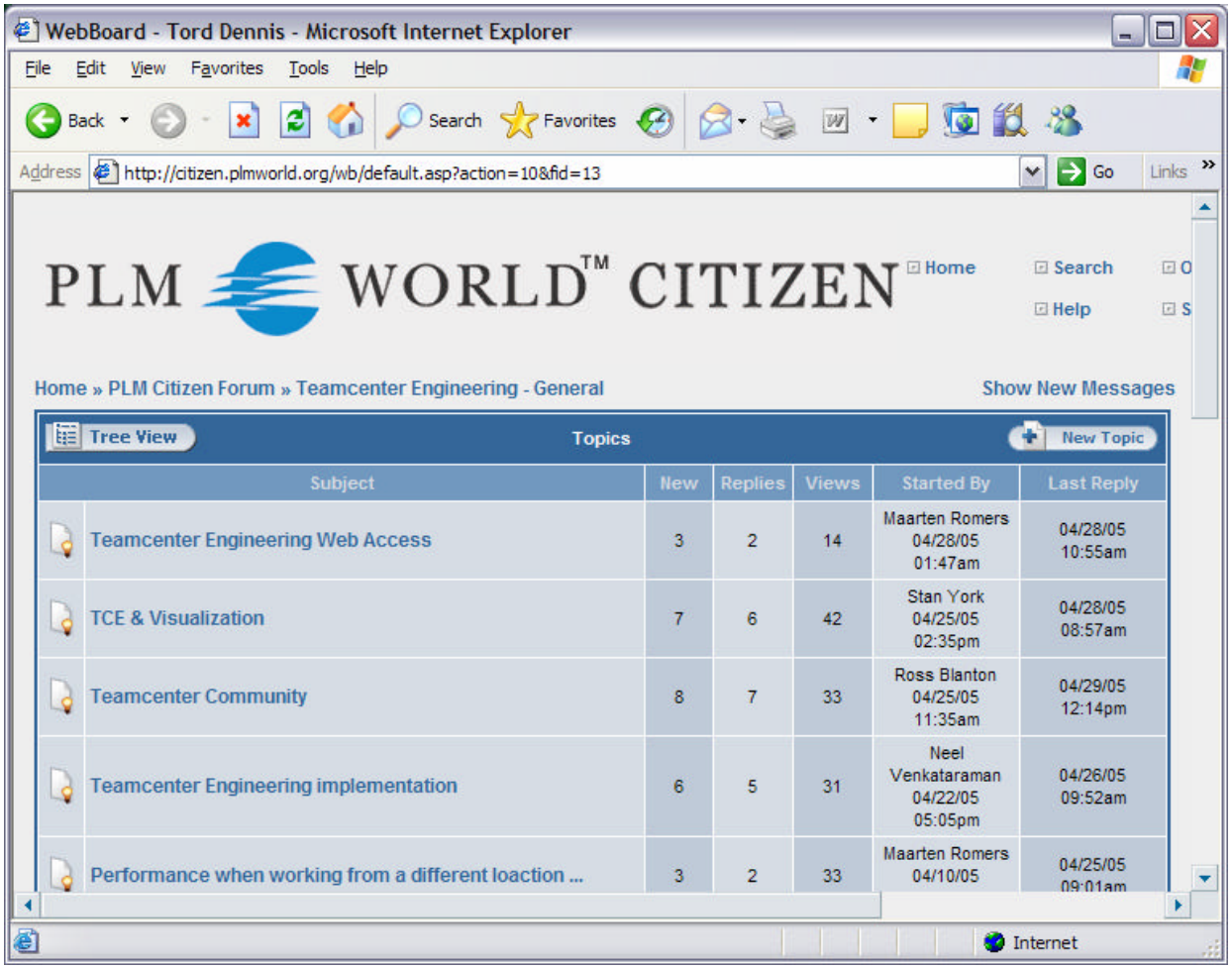
tdennis@cad.gatech.edu

Stateful firewalls

A stateful firewall is able to hold in memory significant attributes of each connection, from start to finish. These attributes, which are collectively known as the state of the connection, may include such details the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection. The most CPU intensive checking is performed at the time of setup of the connection. **All packets after that (for that session) are processed rapidly because it is simple and fast to determine whether it belongs to an existing, pre-screened session.** Once the session has ended, its entry in the state-table is discarded.

http://en.wikipedia.org/wiki/Stateful_firewall

Getting Help Globally



tdennis@cad.gatech.edu

Getting Help Locally

tdennis@cad.gatech.edu

Future work

Just because you're paranoid, it doesn't mean they're NOT out to get you.

- Teamcenter Engineering 9 & NX Manager
  - Firewalls are a necessary evil!
  - Don’t fear Oracle
- NX3 & Solid Edge

Wish List

- Teamcenter Community
- Non-UGS CAD management

tdennis@cad.gatech.edu

Questions

Tord Dennis
Research Engineer
College of Engineering
Georgia Institute of Technology
tdennis@cad.gatech.edu
404.894.7752

Technical Track: Academia

Managing student projects in a collaborative environment using Teamcenter Engineering

Wednesday, 4:00 PM