Idaho National Laboratory

INL Assessment Team On-Site General Findings

Highlight Report

Assessment Team Members:

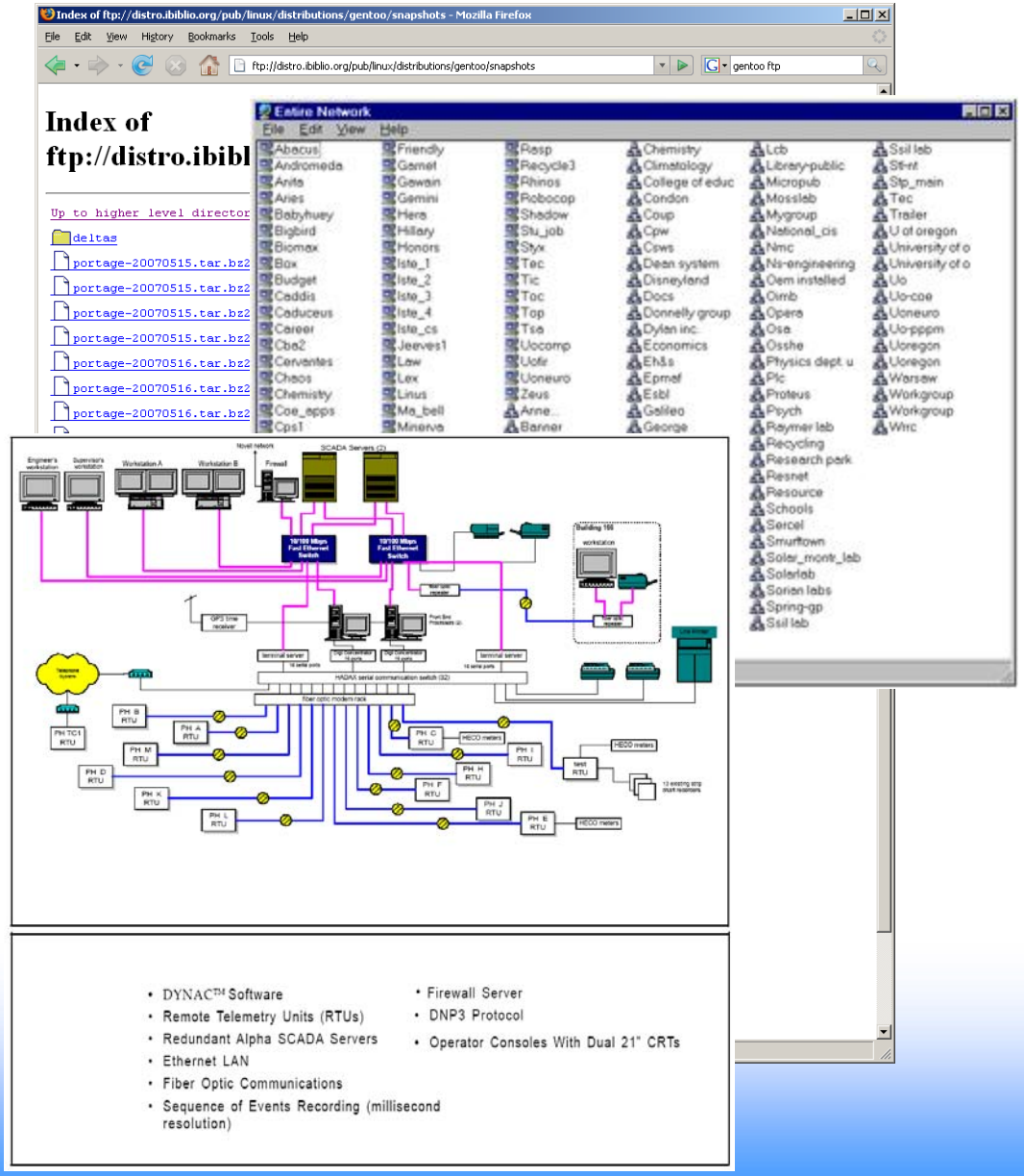
Shane Hansen
James Lee
Michael Milvich
Ken Rohde
Steve Schaeffer
Jared Verba

Introduction

- **Over the past 18-20 months, 13 on-site assessments conducted**
- **Sites included: generation, distribution, and water**
- **Assessments included most of the major SCADA and/or DCS vendors**
- **The findings in this presentation are more common than you might think…**

Information Disclosure

- Web Servers
- Engineering Systems
- FTP Servers
- Samba Shares
- Development / Quality Systems



Idaho National Laboratory

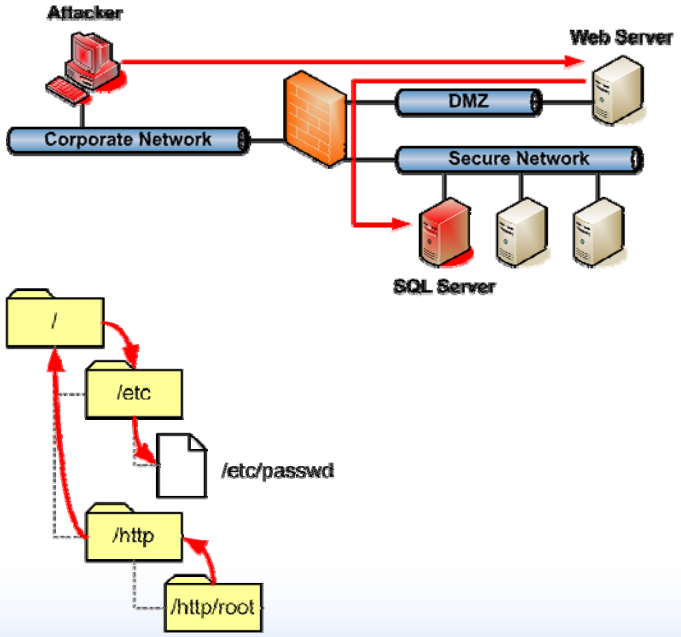
Custom Applications

Including:

- **Web Applications**
- **Data Converters and Exchange**
- **Plugins**
- **Anything developed internally or for internal use**

Common Problems:

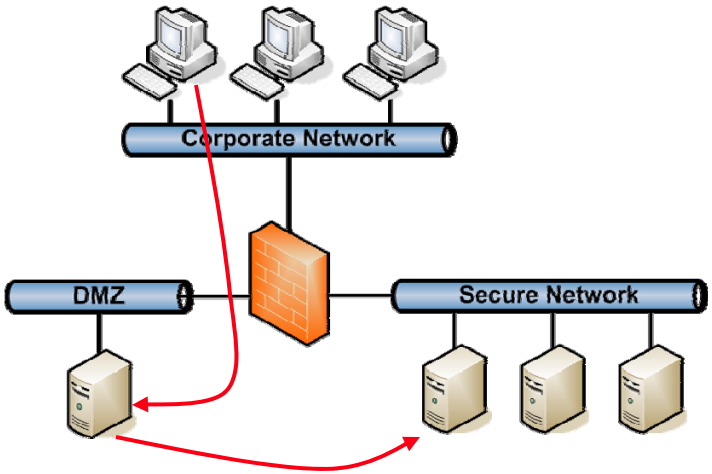
- **Clear Text Authentication**
- **Client Side Authentication**
- **Backend Services Accounts**
- **SQL Injections**
- **Directory Traversals**
- **Buffer Overflows**

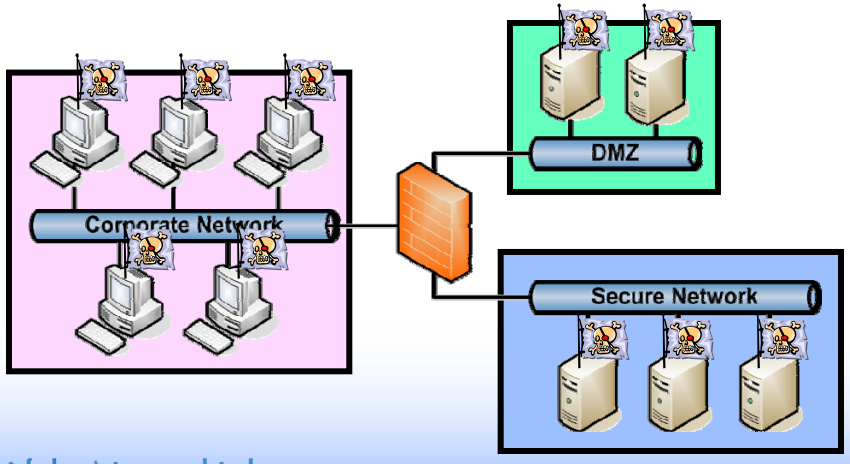


Bad Passwords

(Yes, this is the obligatory section on bad passwords)

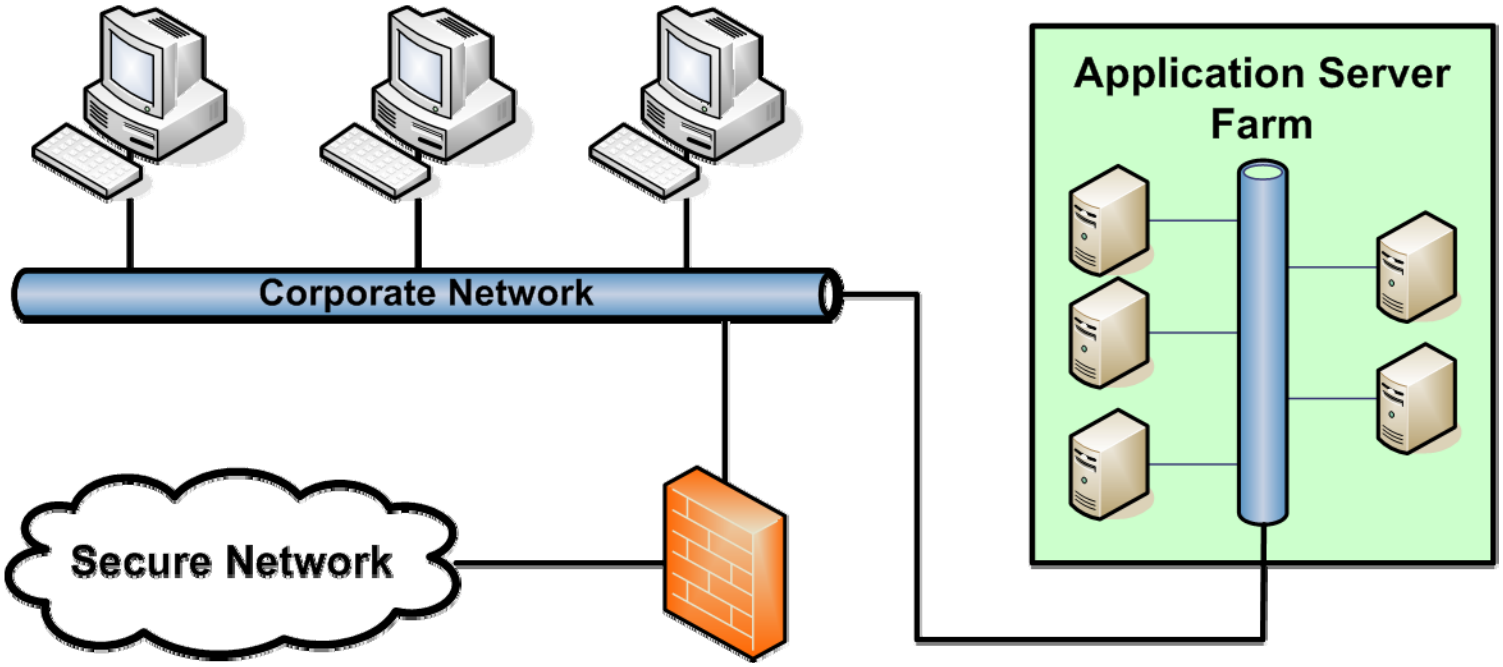
- **Outward Facing Services**
- **Just Plain Bad Passwords**
- **Homogeneous Passwords**
- **Backend Service Accounts**
- **LANMAN**
- **Default Accounts**





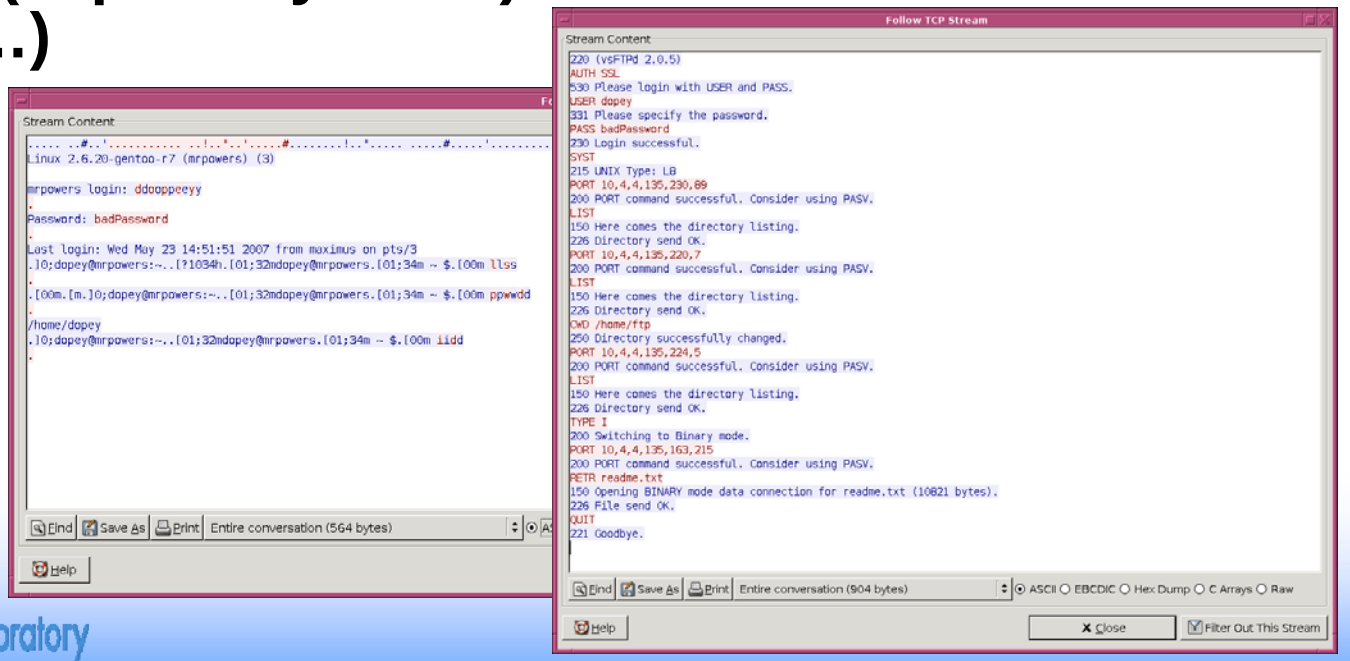
Application Servers

- **Corporate Clients need data from the secure network.**



Unsafe / Unneeded Services

- **Reliance upon and/or not knowing if needed**
- **Replacement options *are* reasonable**
- **Several guides available for disabling services on Windows platforms (NIST.gov, governmentsecurity.org, …)**
- ***nix systems (especially older) need to be checked (netstat, ps, …)**

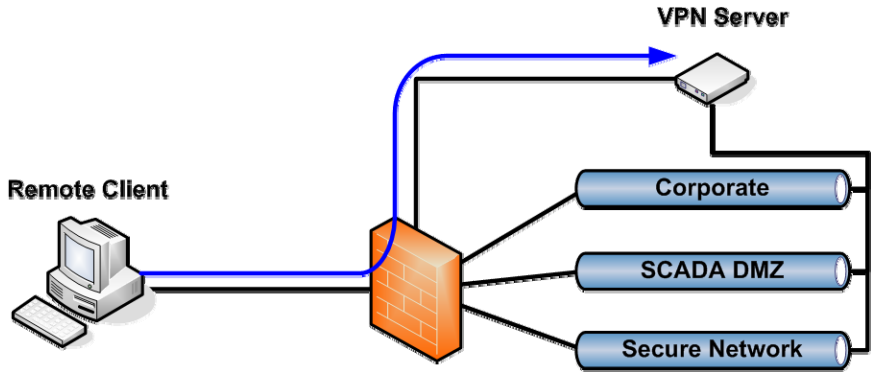


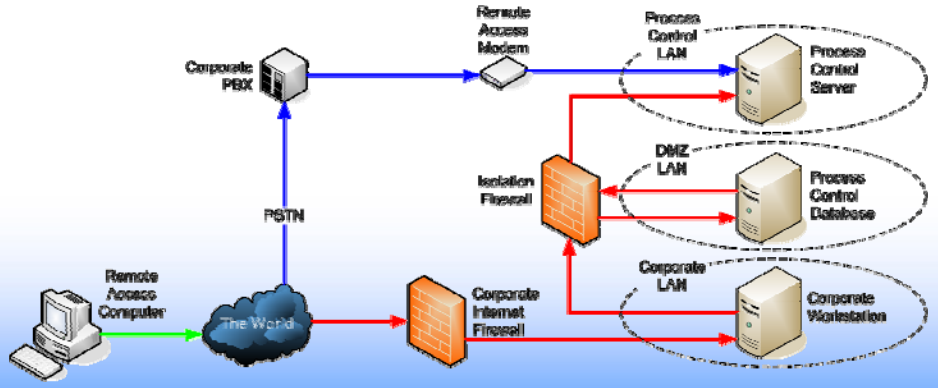
Idaho National Laboratory

Examples: Telnet, FTP, REXEC, RSH, ECHO, Discard

Remote Access

- Backend modems bypass security infrastructure
- Vendor VPN access
- Engineering access
- Client side access rights
- IT access





Idaho National Laboratory

Firewalls & Intrusion Detection

Firewalls:

- Huge rule set and complex rules
- Generic or simplified rules
- Old/temporary rules not removed
- Rules exist, but nobody knows why
- Logging not enabled
- Firewall is subverted by direct connection

IDS/IPS:

- New to control industry as a whole
- Not even employed at corporate level
- Seldom audited or tested
- Sometimes deployed but not “enabled”
- Hardware capabilities often fall short
- Log correlation seldom used
- Alert level is high (false positives) so most alerts are ignored