



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

The top part of the image shows a screenshot of a Mozilla Firefox browser window displaying the index of an FTP site: `ftp://distro.ibiblib.org/pub/linux/distributions/gentoo/snapshots`. The page lists various directory listings and files, including several `portage-20070515.tar.bz2` and `portage-20070516.tar.bz2` files. An 'Entire Network' window is overlaid on the browser, showing a grid of network shares with names like 'Abacus', 'Andromeda', 'Anife', etc.

The bottom part of the image shows a detailed network diagram. It illustrates a complex system with multiple workstations (Engineer's workstation, Supervisor's workstation, Workstation A, Workstation B), SCADA servers, and various communication protocols. Key components include a '20100 Mbps Full Ethernet Switch', '20100 Mbps Full Ethernet Switch', 'Serial server', 'Modem rack', and numerous Remote Telemetry Units (RTUs) labeled PH A through PH L. The diagram also shows connections to a 'Building 106' and various servers and databases.

- DYNAC™ Software
- Remote Telemetry Units (RTUs)
- Redundant Alpha SCADA Servers
- Ethernet LAN
- Fiber Optic Communications
- Sequence of Events Recording (millisecond resolution)
- Firewall Server
- DNP3 Protocol
- Operator Consoles With Dual 21" CRTs

Custom Applications

Including:

Web Applications

Data Converters and Exchange

Plugins

Anything developed internally or for internal use

Common Problems:

Clear Text Authentication

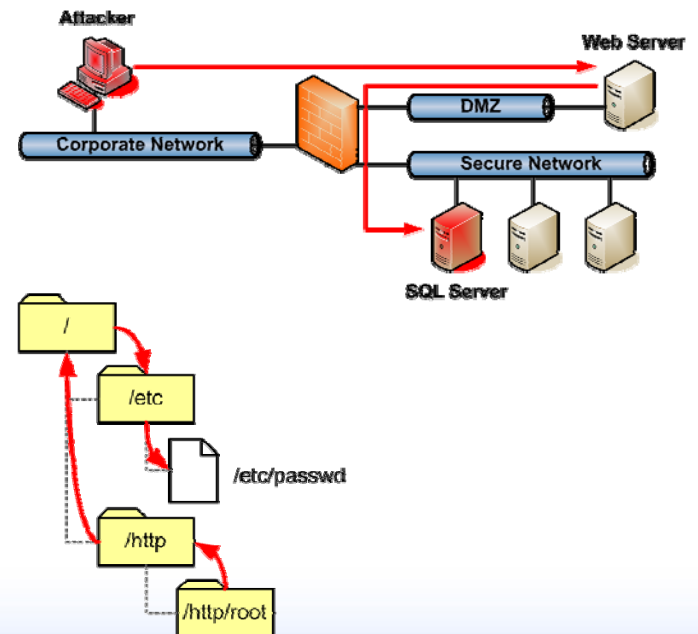
Client Side Authentication

Backend Services Accounts

SQL Injections

Directory Traversals

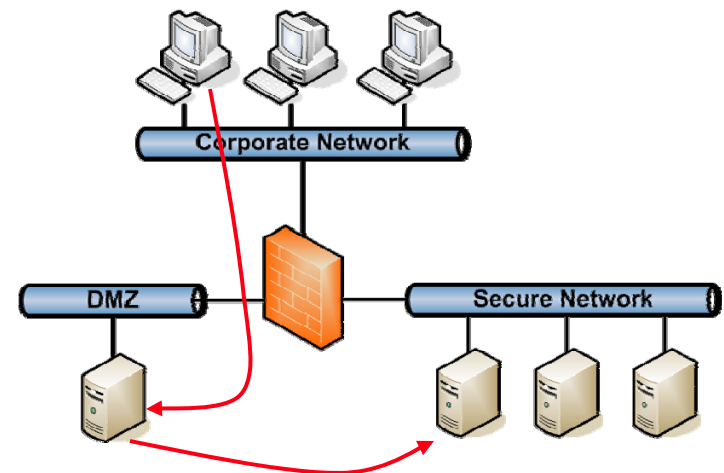
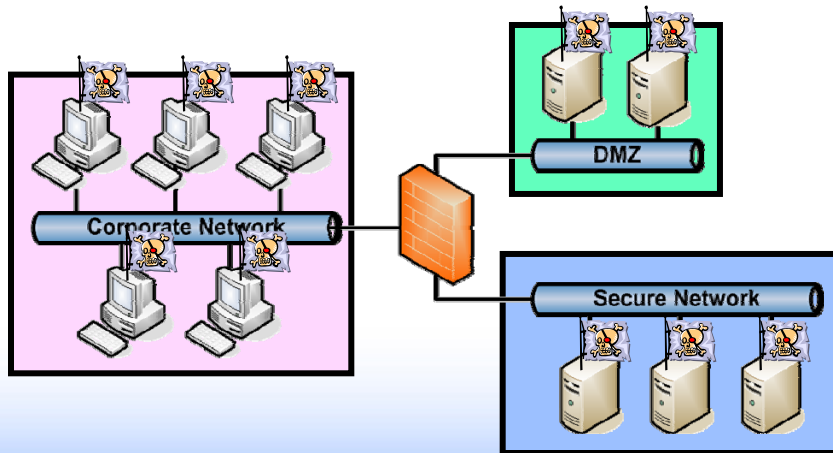
Buffer Overflows



Bad Passwords

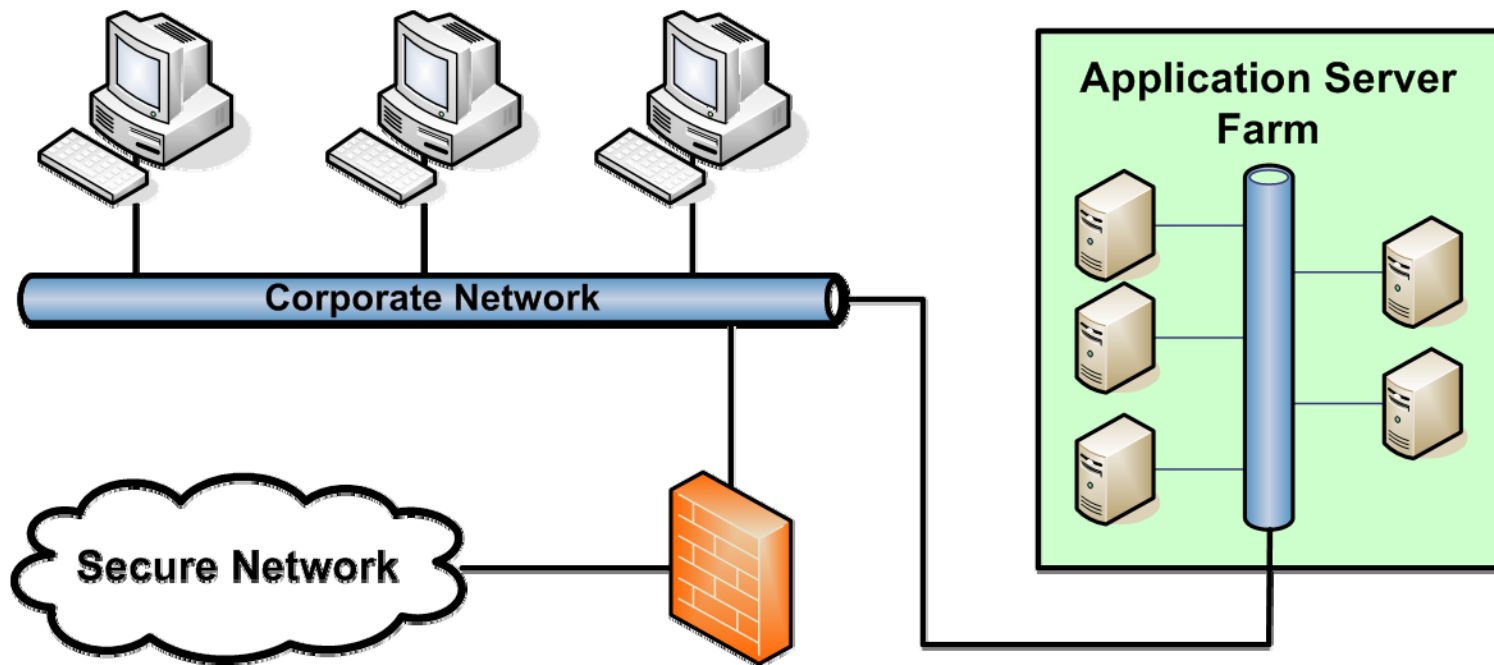
(Yes, this is the obligatory section on bad passwords)

- 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, ...)

```
Linux 2.6.20-gentoo-r7 (mrpowers) (3)
mrpowers login: ddoappeey
Password: badPassword
Last login: Wed May 23 14:51:51 2007 from maximus on pts/3
.10;dopey@mrpowers:~$ ?1634h.[01;32ndopey@mrpowers.[01;34m ~ $.[00m llss
.[00m.[m.]0;dopey@mrpowers:~$.[01;32ndopey@mrpowers.[01;34m ~ $.[00m ppwdd
/home/dopey
.10;dopey@mrpowers:~$.[01;32ndopey@mrpowers.[01;34m ~ $.[00m lidd
```

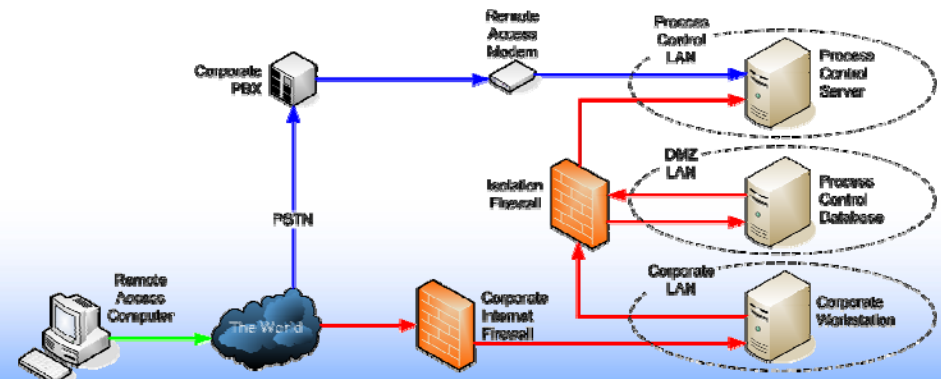
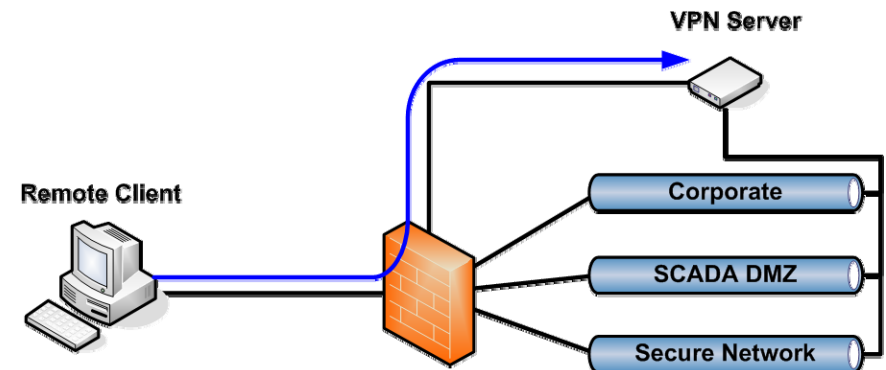
```
Stream Content
220 (vsFTPd 2.0.5)
AUTH SSL
530 Please login with USER and PASS.
USER dopey
331 Please specify the password.
PASS badPassword
230 Login successful.
SYST
215 UNIX Type: L8
PORT 10,4,4,135,230,89
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
PORT 10,4,4,135,220,7
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
CWD /home/ftp
250 Directory successfully changed.
PORT 10,4,4,135,224,5
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 10,4,4,135,163,215
200 PORT command successful. Consider using PASV.
RETR readme.txt
150 Opening BINARY mode data connection for readme.txt (10821 bytes).
226 File send OK.
QUIT
221 Goodbye.
```



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



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**