Critical Alert for Cyber Terror

WHITE PAPER

Security for Nation’s Infrastructure (SCADA & DCS)

© Copyright 2002 sanghun, Jeon. All rights reserved.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Contents</td>
<td>4</td>
</tr>
<tr>
<td>CONTENTS</td>
<td>6</td>
</tr>
<tr>
<td>Infra Structure Control System</td>
<td>13</td>
</tr>
<tr>
<td>±â¹Ý½Ã¼³Á¦¾î½Ã½ºÅÛº¸¾È</td>
<td>20</td>
</tr>
<tr>
<td>SIMULATION</td>
<td>23</td>
</tr>
<tr>
<td>Cyber Attack simulation</td>
<td>23</td>
</tr>
<tr>
<td>SECURITY PLAN</td>
<td>25</td>
</tr>
<tr>
<td>Security Policy</td>
<td>25</td>
</tr>
<tr>
<td>Security Technic</td>
<td>25</td>
</tr>
<tr>
<td>Security for Future</td>
<td>26</td>
</tr>
<tr>
<td>REFERENCE</td>
<td>27</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>28</td>
</tr>
<tr>
<td>ABOUT MY LIFE</td>
<td>29</td>
</tr>
</tbody>
</table>
2002 年 9 月 20 日 宣示國家戰略《安全的網路空間》 "The national strategy To SECURE CYBER SPACE"，"Cyber"SCADA system DCS.

¹ßÀüµÇ°í ±Û·Î¹ú ³×Æ®¿öÅ©¸¦ ÀÌ·ç±â À§Çؼ­´Â ³×Æ®¿öÅ©¸¦ ±¸¼ºÇÏ´Â °¢ ¿ä¼Ò¿¡ ´ëÇÑ ð§½Å¼ÓÇÑ ð§º¸¾È°¡À̵尡 Àý½ÇÈ÷ ÇÊ¿äÇϸç »ýȰ °ú »çȸÀÇ Á¸¸³±â¹Ý°ú ´ÐÁ¢ÇÑ ¿¬°üÀ» °¡Áö°í ÀÖ´Â ±â¹Ý½Ã¼³¿¡ ´ëÇÑ ð§º¸¾ÈÀº ð§º¸´Ù ´õ öÀúÇÑ ð§º¸¾È°ú °¢ À§Çè¿ä¼Ò¿¡ ´ëÇÑ ÀÎÁö¿Í ´ëºñÃ¥ ±×¸®°í ¿ÀÇÁ¶óÀÎ »óÀÇ ºñ»ó»çÅ¿¡ ´ëÇÑ º¹±¸Ã¥»Ó¸¸ ¾Æ´Ï¶ó ÀÎÁö¿Í. 
## Contents

### Vulnerability Report

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>171</td>
<td>345</td>
<td>311</td>
<td>262</td>
<td>417</td>
<td>1,090</td>
<td>2,437</td>
<td>3,222</td>
</tr>
</tbody>
</table>

* 2002 Q1-Q3: 9

- www.cert.org
Year | Incidents reported
--- | ---
1988 | 6
1989 | 132
1990 | 252
1991 | 406
1992 | 773
1993 | 1334
1994 | 2340
1995 | 2412
1996 | 2573
1997 | 2134
1998 | 3734
1999 | 9869
2000 | 21576
2001 | 54658
2002 (Q1~Q3) | 73359
2002 CSI/FBI Computer Crime and Security Survey

Insider Attacks
Outsider Attacks

2002 CSI/FBI Computer Crime and Security Survey
1 - Sample Home Automation
2 - Sample Home Automation Network

Home Network

Home Automation

Home Server: TCP/IP, RF, PLC, ARS

Home Gateway: TCP/IP, RF, PLC, ARS
Web Pad: アイデアを共有し、あらゆる業種で持続可能な社会を作り出すためのツール

* Web Padは、Webを駆動するトータルソリューション・システムとして、TCP/IPを使用してデータを送受信する。

IT業界では、インターネットが広く利用されている。

交通機関、電力供給、産業、建設業界など、あらゆる業界でWeb Padを活用しています。
WS: Work Station – Factory Automation, Computer Integrated Manufacturing

EWS: Engineering Work Station, WS, FA

Control system

Main Server 1  Main Server 2

TCP/IP  OR  Private Line

Local 1

Local 2

Local 3
Counterterrorism analysts have known for years that terrorists often prepare for attacks with elaborate "targeting packages" of photographs and notes. But, in January, U.S. forces in Kabul, Afghanistan, found something new. A computer seized at an al Qaeda office contained models of a dam, made with structural architecture and engineering software, that enabled the planners to simulate its catastrophic failure. Bush administration officials, who discussed the find, declined to say whether they had identified a specific dam as a target. The FBI reported that the computer had been running Microstran, an advanced tool for analyzing steel and concrete structures; Autocad 2000, which manipulates technical drawings in two or three dimensions; and software "used to identify and classify soils," which would assist in predicting the course of a wall of water surging downstream. To destroy a dam physically would require...
"tons of explosives," Assistant Attorney General Michael Chertoff said a year ago. To breach it from cyberspace is not out of the question.


2. In 1998, a 12-year-old hacker, exploring on a lark, broke into the computer system that runs Arizona's Roosevelt Dam. He did not know or care, but federal authorities said he had complete command of the SCADA system controlling the dam's massive floodgates. Roosevelt Dam holds back as much as 1.5 million acre-feet of water, or 489 trillion gallons. That volume could theoretically cover the city of Phoenix, down river, to a height of five feet.

http://www.itsa.org/ITSNEWS.NSF/4e0650bef6193b3e852562350056a3a7/3f141fc26dcebd5a85256be600617016?OpenDocument

3. In Queensland, Australia, on April 23, 2000, police stopped a car and found a stolen computer and radio transmitter inside. Using commercially available technology, Vitek Boden, 48, had turned his vehicle into a pirate command center for sewage treatment. Boden's arrest solved a mystery that had troubled the area's wastewater system for two months. Somehow the system was leaking hundreds of thousands of gallons of putrid sludge into parks, rivers and commercial properties. Until Boden's capture -- during his 46th successful intrusion -- the utility's managers did not know why. Specialists in cyber-terrorism have studied Boden's case because it is the only one known in which someone used a digital control system deliberately to cause harm.

http://www.theregister.co.uk/content/4/22579.html
Infra Structure Control system

SCADA (Supervisory Control and Data Acquisition)
MODICON (Modular Digital Controller) has RS-485, ABB, and PC connections. PLC (Programmable Logic Controller) has Control PC connections. Control PC controls PLC.
1. SCADA, DCS, Utility, Tool, ...  

1. SCADA, DCS, Utility, Tool, ...  

2. SCADA, DCS, Utility, Tool, ...  

3. SCADA, DCS, Utility, Tool, ...
Remote management tool

IDC (Internet Data Center)

2~3

Back

Orifice, Net bus, Netcat, Key Logger

4.

http://www.hani.co.kr/section-005000000/2002/10/005000000200210142158142.html
1. SCADA

2. SCADA

3. SCADA
1. Web site

2. DNS Server

3. FTP, WEB, Mail Server

4. IDS, VPN

5. SCADA

A. User Interface

B. SCADA
SCADA

1. SCADA ¿½ÅÛÀº ±¸Ãà ÀÎÁõ¿¡ µÇ¾î ÀÌ¿¡ µû¸¥ °í·ÁºÎ Á·ÇÑ°¡°í ÀÖÀ¸¹Ç·Î ±â´ÉÀ» Á¡Á¡ ¼³°è

2. RTU ¡ IED ¡ IP ¡ UCA/MMS & DNP ¡ OSI ¡ TCP/IP ¡ PLC ¡ Utility Protocol (ex. UCA/MMS & DNP)

RTU: remote terminal unit
IED: Intelligent Electronic Device
UCA: Utility communication Architecture
MMS: Manufacturing Message Specifications
DNP: Distributed Network Protocol
OSI: Open Systems Interconnection
TCP/IP: Transmission Control Protocol/Internet Protocol
PLC: Programmable Logic Controller


4. Legacy (ex. UCA/MMS & DNP)

5. Legacy
Cyber Attack simulation

1. DMZ [DMZ][Webserver][Mail Server] [IP][Internal Network][DMZ][Internal Firewall][SCADA]
   [DMZ][Sniffer][Internal Firewall][DB][PC][Hacker]

2. [DMZ][Hacker][Web Server][Mail Server][Internal Firewall] [DMZ][DB Server][Hacker]
   [DMZ][SCADA]
3. DMZ

SCADA system

PLC (Programmable Logic Controller)

PLC
Security Plan

Security Policy

1. Cyber Terror
2. Cyber war
3. ...
4. ...
5. ...
6. ...
7. ...
8. ...
9. ...
10. ...
11. ...

Security Technic

DMZ
VPN
LOCKING
SCADA

Virus:

i. Anomaly Detection
   Heuristic Logic
ii. 
iii. Gateway
iv. 
i. IDS, Firewall, Router
ii. ESM

Security for Future

1. 1, 2
2. Security
3. ESM
4. 1, 2
5. Managed Security
6. 1, 2
References

   “Security experts weigh in on cybersecurity plan” By Paul Roberts, IDG News Service, 09/18/02

   "Security experts weigh in on cybersecurity plan" By Paul Roberts , IDG News Service, 09/18/02

   “Cyberspace: The next battlefield “ By Andrea Stone, USA TODAY

   “California hack points to possible IT surveillance threat” DAN VERTON June.12 2001

   “Feds, Industry, Battle the Biggest Bug” Kevin Poulsen, Jun 12 2002 12:00AM

   “U.S. Fears Al Qaeda Cyber Attacks” Barton Gellman, Washington Post Jun 26 2002 3:59PM

7. http://www.itsa.org/ITSNEWS.NSF/4e0650bef6193b3e852562350056a3a7/3f141fc26dceb5a85256be600617016?OpenDocument
   “Internet-Based And Remotely-Controlled Public Infrastructure And Utility Networks More Vulnerable Than Previously Thought “ June 28, 2002

8. http://www.theregister.co.uk/content/4/22579.html
Bibliography

“The National strategy to SECURE CYBER SPACE” September, 2002  The President’s Critical Infrastructure Protection board
http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf

“Real time Information Protection” Riptech technology.

“Securing supervisory control & data acquisition”  Abdo Y.saad ,M.S
http://www.undergroundinfo.com/PGI/pgj_archive/July02articles/securingsupervisory.pdf

“Common Vulnerabilities in Operational Networks”  Riptech technology

“SCADA Security Stratege”, Jonathan Pollet, PlantData Technologies  August 8, 2002

About My Life

[Text content]

© 2023 [Author]. All rights reserved.

[End of text]