군 사 과 학 연 구 지
제14권 제1호(2021년 6월)

북한 운영체제 붉은별의 응용 소프트웨어 분석

An Analysis of Redstar Application Software in North Korea Operating System

류효진[1] · 강동수[2]
Hyojin Ryu · Dongsu Kang

ABSTRACT

North Korea has pursued policies to reinforce science and technology. Specifically, North Korea regards its software industry as a strategic industry. North Korea faces a military confrontation with South Korea. Simultaneously, it is a market with great potential for software industry. Therefore, Republic of Korea not only makes a effort to respond to North Korea's cyber threats, but also continues to discuss civilian-level information technology cooperation. In this regard, it is necessary and crucial to obtain the information on software technology and cyber-security system. In addition, it is needed to analyze the level of information technology service in North Korea. This study provides context to the information related to North Korea's software such as detailed functions and security system through analysis of the Redstar, an operating system developed by North Korea. As a result, we will be able to figure out the current state of North Korea's software technology and utilize it as basic data for research on Redstar.

Key Words: Redstar, North Korea, IT, software, operating system, security

논문접수일 : 2021년 4월 21일, 심사일 : 2021년 5월 10일, 게재확정일 : 2021년 5월 21일
1) 국방대학교 컴퓨터공학전공 석사 학생
2) 국방대학교 컴퓨터공학전공 교수 / 교신저자(Corresponding author)

1. 서 론

북한은 2016년 제7차 당대회의 5대 과제로 과학기술 강국건설을 강조함에 이어, 지난 1월 8차 당대회에서 과학기술을 최선의 방략으로 규정하며, 각 부문의 과학기술 발전 목표들을 언급하고, 과학기술 육성을 위한 정책을 꾸준히 추진하고 있다.

특히 북한은 2000년 이후 IT 산업 등 정보화 사업에 주력하면서 상대적으로 경쟁력 있는 소프트웨어(SW) 산업을 성장전략산업으로 설정하였으며,[1] 소학교 3학년부터 컴퓨터 과목을 의무교육으로 지정하고, 김일성종합대학과 김책공업대학, 지방대학에 SW 학부를 신설하는[2] 등 인재 양성을 위한 정책을 추진해왔다.

이를 토대로 김일성종합대학과 김책공업대학 학생들은 2013년부터 세계적 권위의 코딩 경연대회인 코드셰프(CodeChef)에 참가해 지금까지 17차례 이상 우승한 바 있으며, 2018년 전국 정보화 성과 전람회에서는 대만제 회사 가상현실제품(HTC VIVE VR system)에 자체 개발한 SW을 탑재하여 선보이고,[3] 디지털사진기로 입력한 문서화상을 텍스트로 자동변환할 수 있는 문자인식 SW를 개발하여 상용화하는[4] 등 다수의 SW를 자체 개발하여 활용하는 수준에 이르렀다.

이처럼 국가 차원에서 SW 산업을 육성하고 있는 북한은 우리와 군사적으로 대치하고 있는 존재이며, 한편으로는 신기술산업에서 잠재력이 큰 시장이기도 하다. 그로 인해 국내에서는 '해킹 피해 예방을 위한 북한 등 해킹수법 정보 공개법'을 발의하는 등 북한 사이버 위협에 대응하기 위한 노력과 동시에 정보통신정책연구원(KISDI), 동북아 공동체 ICT(Information and Communication Technologies) 포럼에서 민간 차원의 남북 ICT 교류 협력을 위한 논의를 지속하였으며, 특히 초기 인프라 투자 소요가 적은 SW 협력이 주목받고 있다.

이러한 측면에서 북한의 SW 기술과 보안체계에 대한 지속적인 정보 획득이 선행되어야 하며, 이를 바탕으로 북한의 정보화 수준에 대한 분석 및 관찰이 필요하다.

본 연구의 첫 번째 목적은 북한이 자체 개발한 운영체제 붉은별(Redstar) 분석을 통해 북한 SW 세부 기능 및 보안체계와 관련한 정보를 살펴보는 것이다. 이를 통해 북한 SW 기술의 현주소를 이해할 수 있을 것이며, 붉은별 연구를 위한 기초자료로 활용할 수 있을 것이다.

두 번째 목적은 붉은별 기존 연구들과 북한 SW 개발 동향을 통해 시사점을 도출하는 것이며, 이를 기반으로 북한의 사이버 위협에 대응하기 위한 정책을 제언한다.

본 논문의 구성은 다음과 같다. 제2장은 붉은별 기존 연구를 소개하고, 제3장에서는 붉은별의 주요 응용 SW와 세부 기능을 소개하여 이를 바탕으로 북한 SW 수준과 개발 중점을 도출한다. 또한 붉은별의 보안 프로그램과 보안정책을 바탕으로 북한 SW 보안 중점 및 보안체계를 분석한다. 제4장에서는 시사점과 정책을 제언하고, 마지막으로 제5장에서 결론 및 향후 연구를 제시한다.

2. 관련 연구

북한 붉은별 OS가 2008년 처음 등장한 이후, 10여 년의 시간이 흘렀음에도 불구하고 관련 연구가 다방면으로 진행되지 않아 기초자료가 부족한 상황이다. 일부 연구들은 붉은별 등장 초기에 붉은별 1.0과 2.0 버전의 시스템 제원과 SW 기능, 사용자 관점의 특징을 소개하였다.[5, 6]

붉은별 3.0을 분석한 최근 연구들은 다음과 같이 보안 취약점과 워터마킹, 침입탐지 시스템 등 보안 측면에 집중하였다.

붉은별의 보안 취약점을 분석한 연구는 붉은별의 기반이 되는 리눅스(Linux) 버전(2.6.38) 커널의 보안 취약점을 CVE(Common Vulnerabilities and Exposures) 목록을 바탕으로 분석하였다.[7]

또한 붉은별 서광사무처리의 보안 취약점을 분석한 연구들은 취약점 식별을 위해 DOM (Document Object Model)을 기반으로 한 파일 퍼징(Fuzzing) 기법을 제안했고,[8] 서광사무처리의 파일 구조인 ODF(Open Document Format)와 XML(Extensible Markup Language)의 취약점을 CVE를 통해 분석하였다.[9]

그 외에도 붉은별 3.0의 보안 기능 중 하나인 워터마킹을 이용한 비가시적(Invisible)인 정보은닉 방법과[10] 붉은별의 침입탐지시스템 Snort의 탐지 규칙을 분석하여 폐쇄적인 감시 시스템이 더욱 강화되었음을 증명한 연구가 [11] 있다.

3. 붉은별 응용 SW 분석

3.1 붉은별의 기본정보

붉은별은 북한의 SW 개발기관인 조선콤퓨터쎈타(KCC, Korea Computer Center)가 개발한 리눅스 기반의 체계로, <표 1>과 같이 버전별로 개발되었다.[12]

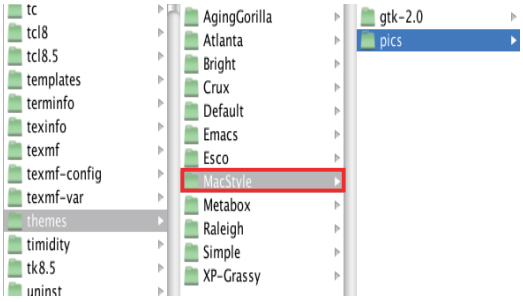
북한은 1990년 KCC 설립 이후 많은 기관들과 공동연구를 통해 2008년 붉은별 1.0을 독자적으로 개발하였고, 2009년에 2.0, 2012년에 3.0버전을 개발하였다. 2017년에는 대외선전매체 홈페이지를 통해 28차 전국 정보기술 성과 전시회 소개 영상에서 정보화 사업의 일환으로 붉은별 4.0을 개발했다고 공표하였다.[9]

붉은별은 리눅스에서 윈도우 프로그램을 사용할 수 있게 하는 KDE(Kool Desktop Environment)를 기반으로 하며, 오피스 프로그램인 우리와 서광, 바이러스 백신 및 보안 강화 프로그램들이 설치되어 있다. 또한, 한글 지원을 개발하여 사용자에게 편리한 환경을 제공한다.

<표 1> 붉은별 운영체제 개발 현황

버전 (연도)	커널 버전	Application SW
1.0 (2008)	Red Hat 4.1	Crosswin Anti-Virus URI Office
2.0 (2009)	Linux 2.6.25-14	Mannung Anti-Virus (Clacksae) Seogwang Office 2.0 Byungjin1.0(calculation) Pado2.0 (file transport) Bydukgi (e-mail)
3.0 (2012)	Linux 2.6.38	Bogem Seogwang Office 3.0 Unbangul Task Manager SCNPRC
4.0 (2015)	Ubuntu 12.04.2	Seogwang Office 4.0 Virtual Box Modemcom 등 Application 37개

붉은별 1.0과 2.0의 구성은 윈도우와 유사하지만, 붉은별 3.0부터의 UI(User Interface)는 맥 OS를 모방하고 있다.[8] 붉은별 파일탐색기 themes에 <그림 1>과 같이 MacStyle이 명시되어 있다.

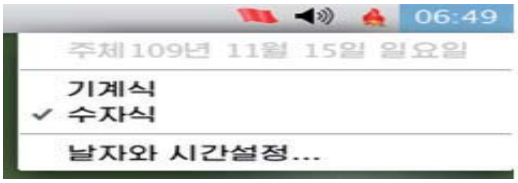


<그림 1> 붉은별 3.0 themes의 MacStyle

우리와 다른 북한의 특징적인 모습은 사용 언어와 시간 표기 방법에서 찾아볼 수 있는데, <표 2>와 같이 우리와 다른 용어를 사용하고 있으며, 그 외에 외래어 사용으로는 콤퓨터, 싸이트, 쏘프트웨어, 로긴, PDF, 마우스 등이 있다. 또한 <그림 2>처럼 실행화면 오른쪽 시간 표기를 주체 109년과 같이 북한식으로 표현한다.

<표 2> 윈도우 한글버전과 붉은별 용어 차이

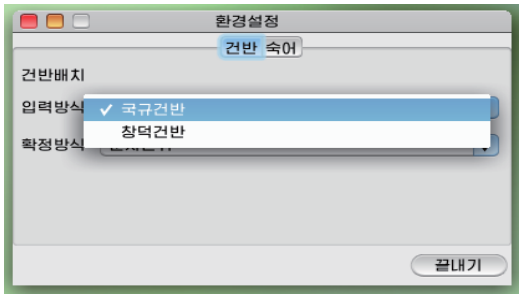
윈도우 한글버전	붉은별
바탕화면	탁상화면
미디어 플레이어 (Media Player)	다매체 재생기
윈도우 시작	대화접속기
패스워드(Password)	통과암호
바이러스(Virus)	비루스
페이지읽기 오류	페지읽기오유
작업관리자	동태감시기
재시작	재기동
로그오프(Log-off)	가입취소
즐겨찾기	root의 서류절
명령프롬프트(CMD)	조작탁
웹브라우저 (Web Browser)	내나라 열람기
계산기	전자수산기
서버(Server)	봉사기
키보드	건반
네트워크(Network)	망
단축키	건반지름건



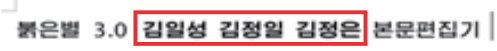
<그림 2> 북한식 시간 표기법

다른 특징으로 붉은별은 북한식 키보드 입력방식인 국규건반이 기본값이기 때문에 우리가 쓰는 두벌식 키보드로는 문장 입력이 제한된다. 그러나 <그림 3>과 같이 창덕건반으로 바꾸면 우리의 키보드 배열을 그대로 사용할 수 있다.

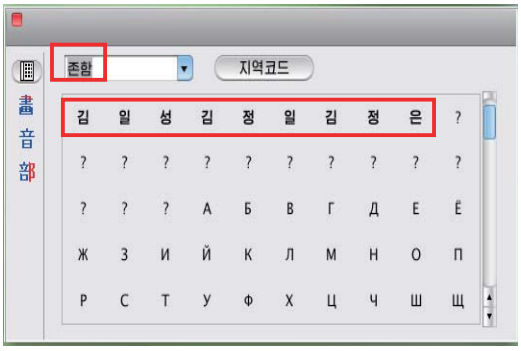
또한, 붉은별에서 김일성, 김정일, 김정은을 입력하면, <그림 4>와 같이 자동으로 해당 글자가 굵게 처리된다. 이는 <그림 5>에서 볼 수 있듯이 김, 일, 성, 김, 정, 일, 김, 정, 은과 같은 문자가 존함 항목에 특수문자로 등록되어 있기 때문이다. 즉, 북한 전·현직 지도자 이름을 굵게 하여 도드라지게 표시하는 것이 북한의 표기법이라고 볼 수 있다.



<그림 3> 키보드 입력방식 변경



<그림 4> 특정 단어 입력시 자동 볼드(Bold)체 변환



<그림 5> 특수문자로 등록된 북한 전·현직 지도자 이름

붉은별 1.0과 2.0의 응용 SW는 각각 4개, 15개로 확대되었다.[13] 붉은별 3.0 응용 SW는 23개이며, 그중 일부 SW를 설치한 탑재화면은 <그림 6>과 같다.

<그림 6> 붉은별 3.0 응용 SW 탑재화면

<그림 7> 응용 SW 및 개발도구 선택화면

붉은별 설치 과정에서 <그림 7>과 같이 탑재할 SW 목록을 선별적으로 선택할 수 있다. 이후 붉은별 4.0의 응용 SW는 37개로 증가하였다.

붉은별의 버전별 주요 응용 SW는 <표 3>과 같이 변화하였다. 붉은별 1.0의 오피스 프로그램 우리 1.0과 윈도우 응용 SW 사용을 지원하는 Crosswin이 붉은별 2.0 이후부터 각각 서광과 만능으로 명칭이 변경되었다. 또한 데이터베이스 관리 시스템인 MySQL을 바탕으로 한 자료기지봉사기. 암호화 파일체계 보검, 각종 악보를 연주하고 인쇄할 수 있는 SW인 은방울, C/C++ 프로그램 개발 및 인터페이스 설계도구인 삼태성, JAVA 통합개발을 지원하는 어깨동무와 같은 다양한 기능의 SW들이 추가되었다.

3.2 주요 프로그램

3.2.1 오피스 프로그램 서광사무처리

북한 삼일포정보쎈터에서 개발한 붉은별 1.0의 오피스 프로그램 우리 1.0은 리눅스의 오픈오피스를 기반으로 하고 있으나, 붉은별 2.0은 자체적으로

<표 3> 붉은별 버전별 주요 응용 SW

구 분	1.0	2.0	3.0	기 능
응용 SW	우리 1.0	우리 3.0	서광 3.0	통합사무처리 프로그램 (오피스 프로그램)
		서광 2.0		
	Crosswin	만능 2.0	만능 3.0	윈도우 환경 지원 SW
	-	내동무 2.0	주소록 3.0	주소록 관리 SW
		비둘기 2.0	우편 3.0	전자우편 전송 · 관리 SW
		내나라열람기(Fire Fox)		웹브라우저
		명수 1.0	류경장기 3.0	조선장기와 수풀이
		환상 1.1	환상 1.0	화상 처리 SW
		평양성 2.0	빛발 3.0	- 평양성 : 방화벽 SW - 빛발 : 통합서버관리도구
		은반 1.1	은반 1.0	CD/DVD 쓰기 SW
		-	은방울 1.0	악보 편집, 연주, 인쇄 SW
			자료기지봉사기	MySQL
			삼태성 3.0	C/C++ 프로그램 개발 및 SW 인터페이스 설계도구
			어깨동무 3.0	Java 통합개발환경
			보검	구획 암호화 및 암호화된 가상디스크 제공

개발한 서광사무처리를 탑재하고 있다.[5] 서광사무처리는 글, 선전물, 표, 자료기지로 구성되며 각각 마이크로소프트의 워드, 파워포인트, 엑셀, 액세스와 유사하다.

붉은별 3.0의 서광사무처리에는 수학식과 형판 기능이 추가되었으며, <그림 8>과 같이 본문문서(워드), 자료표(엑셀)와 연시물(파워포인트)로 명칭이 변화되었다. 또한 조선어, 중어를 비롯해 총 153종의 언어로 된 본문을 입력하고 편집할 수 있으며, 수학식, 표, 3차원 도형 등 복잡한 서식이 포함된 형태의 문서들을 쉽게 작성할 수 있다. 그 외에도 MS 오피스 등의 프로그램들과 문서파일을 교환할 수 있으며 PDF(Portable Document Format) 파일로 반출할 수 있다. 수학식은 적분과 같이 복잡한 계산식을 입력할 수 있는 기능을 제공하며, 형판 기능은 파워포인트의 탬플릿과 같은 기능으로 총 25개의 배경을 제공한다.

<그림 8> 붉은별 '서광사무처리'

서광사무처리는 리브레오피스(LibreOffice)를 기반으로 하며, 확장자는 XML 기반인 ODF를 사용한다. ODF 표준은 사용자가 다른 문서를 작성하기 위해 SW를 활용하더라도 공동으로 문서 작성과 열람을 할 수 있도록 마련한 표준으로, OASIS(Organization for the Advancement of Structured Information Standards)에서 표준화하여 2006년에 ISO/IEC에서 국제 표준으로 승인되었다.[8]

3.2.2 웹브라우저 내나라열람기

내나라열람기는 <그림 9>의 웹브라우저를 말하며, 북한식으로 웨브열람기라고 표현한다. 오픈소스 웹브라우저인 모질라 파이어폭스(Mozilla Firefox)를 기반으로 개발되었다.

붉은별의 내나라열람기는 책갈피, 방문기록과 같은 기능이 있으며, 도구 기능에서는 개인 보호방식을 통해 비공개열람으로 설정하여 기록을 보존하지 않는 기능을 제공한다.

<그림 9> 붉은별 내나라열람기

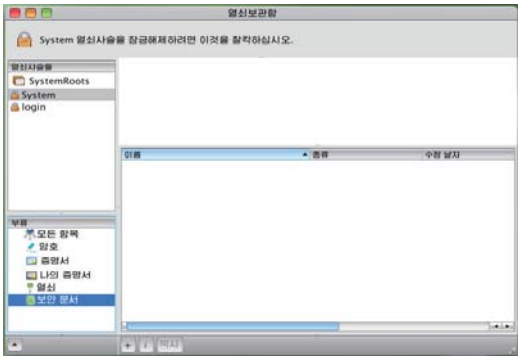
3.2.3 보조 프로그램

붉은별 3.0의 보조 프로그램은 <그림 10>과 같이 동태감시기 등 총 7개이며, 동태감시기는 작업관리자 기능으로써 컴퓨터에서 실행 중인 SW와 프로세스 및 CPU 상의 작업부하를 확인할 수 있다. 디스크편의 프로그램은 SW가 예상치 못하게 완료되거나 파일이 손상되었을 때 파일체계를 수리하며, 구획생성 및 나누기 기능을 제공한다. 체계속성열람기에서 컴퓨터의 하드웨어, SW 및 망에 관한 구체적인 정보들을 열람할 수 있으며, 통합기록열람기에서는 SW 체계 내의 기록들을 제공한다.

사용자는 <그림 11>의 열쇠보관함을 통해 웹사이트, 봉사기, 망, 응용 SW 및 암호화된 등록부나 구동기에 대한 암호와 증명서를 관리할 수 있으며, 열쇠사슬(Keychain) 활용이 가능하다.

열쇠사슬이란 사용자가 기억해야 하는 암호의 개수를 줄이기 위해 열쇠사슬을 사용하는 것을 말한다. 열쇠사슬은 응용 SW, 봉사기, X.509 증명서, 웹사이트에 대한 암호들과 신용카드 번호, 개인식별번호(PIN)와 같은 사용자의 컴퓨터와 무관한 기밀정보를 저장할 수 있다.

<그림 10> 붉은별 3.0 보조SW 탑재화면



<그림 11> '열쇠보관함' 실행화면

망봉사기 접속, 전자우편계정 열람 또는 열쇠사슬과 함께 동작하는 암호로 보호된 항목에 접근시 열쇠사슬이 암호를 제공하므로 별도의 암호를 입력하지 않아도 된다. 표준 열쇠사슬은 처음에 체계 사용자 계정으로 가입시 자동으로 생성되는데, 본인의 계정과 동일한 암호를 가지는 'Login'이라고 하는 열쇠사슬로 시작한다. 해당 열쇠사슬은 계정에 가입하면 자동으로 잠금 해제된다. 다른 용도의 암호들을 저장하기 위해 새로운 열쇠사슬을 생성, 또는 다른 컴퓨터로 가져가기 위해 열쇠사슬을 복사할 수 있다. 한 명의 사용자만 열쇠사슬에 접근이 가능하지만, 컴퓨터의 다른 사용자들과 공유할 수도 있다.

3.3 보안 프로그램 및 정책

3.3.1 바이러스 프로그램

붉은별 1.0의 비루스 왁찐은 북한에서 제작한 바이러스 치료 SW로써 자체적으로 백신 SW를 업그레이드한 흔적들이 있다. 반면, 붉은별 2.0의 백신 SW 클락새는 갱신 기능을 통해 바이러스 회사인 아비라(Avira)의 바이러스 데이터 파일 VDF(Virus Definition Files)를 다운로드 받아 바이러스 리스트를 업그레이드 한다.[13]

3.3.2 보검

보검은 암호화 파일체계로써 구획을 암호화하거나 암호화된 가상디스크를 제공하는 SW로, <그림 12>와 같이 북한의 표준 암호 알고리즘인 필승을 비롯하여 AES, Twofish, Blowfish 등 여러 암호알고리즘을 지원한다. 필승 알고리즘은 Rijndael 암호알고리즘을 기반으로 하며, 미국 NIST(National Institute of Standards and Technology)의 암호화 표준인 AES에 적용된 알고리즘이다.[12]

<그림 12> 붉은별에 사용된 북한의 암호알고리즘

보검에서 제공하는 암호화 매체에는 암호화 구획과 가상디스크가 있다. 암호화 구획은 하드디스크와 USB 디스크와 같은 2차 기억 매체상의 구획을 암호화한 것이며, 가상디스크는 쓰기 가능한 임의의 경로에 지정된 크기의 파일을 만들고 그 내용을 암호화구획처럼 형식화한 것이다. 보검 매체 안에 들어있는 모든 자료, 즉 파일이름, 크기, 속성, 내용, 등록부 구조와 같은 모든 자료는 암호화된다.

3.3.3 SNORT

붉은별 3.0에 설치된 오픈소스 기반의 침입탐지 시스템 Snort는 사용자가 원하는 보안 수준에 맞게 탐지 규칙을 작성할 수 있는 특성이 있다.

붉은별 3.0에서도 일반적인 Snort 탐지 규칙을 수정하였는데, 총 28개의 변수를 추가하였으며 관리자 및 사용자의 권한 탈취 방지, 맬웨어(Malware) 등 공격 탐지를 중점으로 탐지 규칙을 설정하였다. 또한, 패킷 발생량 기반 탐지 규칙은 거의 모든 패킷을 탐지하도록 설정하여 더욱 폐쇄적으로 감시를 강화하고 있다.[11]

3.3.4 워터마킹

북한은 자체 개발한 다양한 모듈과 프로세스를 붉은별에 탑재하였다. 보안과 관련된 커널 모듈은 시스템 및 멀티미디어 파일을 상시 감시하는 RTSCAN(Real Time Scanner)이며, 프로세스는 SCNPRC(바이러스 탐지)와 OPPRC(워터마킹 적용)가 있다. 이들은 많은 라이브러리를 공유하여 멀티미디어 파일을 생성, 복사 또는 수정 시 워터마크를 자동 생성한다.

워터마킹은 디지털 콘텐츠 보안기술 중 하나로, 시각적으로 식별이 어려운 정보를 디지털 데이터에 은닉할 수 있는 기법이다.

붉은별 3.0의 워터마킹은 사람이 지각할 수 없는 비가시성(Invisible)과 연성(Fragile)의 성질을 가진다. 연성 워터마크는 데이터 변형시 워터마크가 쉽게 변형 또는 제거되기 때문에 워터마크를 통해 위·변조 여부를 확인할 수 있는 방법으로, 주로 데이터 무결성 및 인증에 사용된다.

<표 4> 워터마킹이 적용되는 파일 형식

파일종류	형식	파일종류	형식
문서	PPT	이미지	JPG
	DOCX		JPEG
비디오	AVI		BMP
	MP4		GIF

또한, 붉은별 3.0의 워터마킹은 <표 4>와 같이 멀티미디어 파일 중 문서 2종류(PPT, DOCX), 동영상(AVI, MP4), 이미지(JPG, JPEG, BMP, GIF)에 적용된다. 상용 워터마킹과 다르게 파일의 끝에 31바이트의 특정 정보가 태깅(Tagging)되는 방식이며, 16바이트의 가변적인 공간과 15바이트의 고정된 공간으로 구성된다. 가변적인 공간인 16바이트에는 사용자 컴퓨터 하드디스크 일련번호가 DES(Data Encryption Standard) 알고리즘으로 암호화되어 태깅된다.[10]

3.3.5 보안정책

붉은별에는 김책공업대학 조작체계 연구개발센터가 개발한 핵심보안방책 프로그램이 탑재되어 있다. 핵심보안방책 프로그램은 관리자가 시스템의 보안 관련 조사, 분석, 비교 등을 통해 보안을 강화할 수 있도록 지원하며, 사용자의 실행 허가권을 강제로 제어 가능한 SELinux 계열로 개발되었다.[6]

또한 시스템 및 멀티미디어 파일을 상시 감시할 수 있는 RTSCAN 커널 모듈을 자체 개발하는 등 보안 강화를 위해 노력하고 있으며, 그 외에도 OpenSSH(Secure Shell), GPG(Gun Privacy guard)와 같은 오픈소스 방식의 암호화 기술을 도입하였다.

붉은별 3.0에서는 개방 네트워크상에서 인증과 통신의 암호화를 시행하여 보안성을 확보하기 위한 알고리즘인 Kerberos와 VPN(Virtual Private Network), SSO(Single-sign-on)를 적용하며,

방화벽 구축을 위해 iptables를 이용한다.

또한 붉은별 3.0에서는 보안 관리자를 위한 보안 가이드를 통해 보안을 강조하고 있으며, 보안평가 항목과 루트(Root) 암호 관련 요구사항이 <표 5>, <표 6>과 같이 명시되어 있다.

북한은 구체적인 비밀번호 정책으로, 문자나 숫자만으로 이루어진 암호를 사용하지 말아야 하며, 이름이나 사전단어, TV와 책에서 노출되는 단어들로 암호를 구성하는 것을 피해야 하고, 잘 알려진 단어를 거꾸로 한 암호를 사용하지 않도록 강조한다. 또한 암호공격 SW들이 많은 언어를 가진 압축된 사전을 활용하기 때문에 암호로 외국어 단어를 이용하면 안전하지 않다고 밝히고 있다. 이처럼 북한이 체계적으로 보안 정책을 유지하고 있다는 것을 알 수 있다.

<표 5> 붉은별 3.0의 보안평가 항목

구 분	내 용
BIOS, BOOT 보안	- 권한이 없는 사용자들이 물리적으로 접근할 수 있는가? - 단일 사용자 기동인가? - 암호 없이 가능한가?
암호보안	- 사용자 암호를 어떻게 설정하였는가?
관리조종	- 체계관리자가 누구이며 관리조종기능을 얼마나 가지고 있는가?
가능한 서버들	- 망에서 무슨 봉사(서버)들이 있고, 어떤 동작을 하는가?
방화벽	- 방화벽이 어떤 형태인가. 필요한가?
보안 강화된 통신도구	- 어떤 도구들이 통신에 사용되고 있는가? - 보안성능은 어떠한가?

<표 6> 루트 암호 관련 요구사항

구분	내 용
세부 항목	통과암호는 최소한 8문자 이상이어야 한다.
	숫자와 문자가 반드시 결합되어야 한다.
	한 달에 한 번씩 통과암호를 바꾸어야 한다.
	통과암호를 종이에 적어서 보관하는 현상을 없애야 한다.
	통과암호를 작성할 때 어떤 지명이나 이름, 생년월일 등을 피해야 하며, 사전에 없는 문자들로 구성해야 한다.

4. 시사점 및 정책 제언

4.1 시사점

본 연구는 붉은별의 기본정보와 주요 프로그램, 보안 프로그램과 보안 정책들을 분석하여 다음 특징과 시사점을 도출하였다.

첫 번째, SW 개발 측면에서 붉은별 1.0에서 4개였던 응용 SW가 3.0에서 23개, 4.0에서 37개로 확대된 점에서 사용자의 편의성을 높이기 위한 북한의 노력을 엿볼 수 있다. 그러나 북한 네트워크 환경의 폐쇄성으로 인해 오픈소스 기반의 SW들을 사용할 수 없기 때문에 SW 사용의 자유도는 높지 않다고 평가할 수 있다.

두 번째, 북한의 SW 기술은 리눅스를 기반으로 독자적인 SW를 개발하였다는 측면에서 오픈소스를 활용하여 자신들의 환경에 맞게 SW를 최적화할 수 있는 단계로 발전했다고 평가할 수 있다. 하지만 다른 SW와의 호환이 어렵다는 점에서 확대 보급에는 한계가 있을 것으로 판단된다.

세 번째, 붉은별 보안체계에는 북한의 폐쇄성이 반영된 특징적인 보안 요소들이 있다. 붉은별은 리눅스에서 일반적으로 많이 쓰이는 SELinux를 사용하였으나, 이 외에도 자체 개발한 암호화 파일체계인 보검을 적용하였다. 또한 RTSCAN, SCNPRC, OPPRC를 활용하여 보안을 강화하기 위해 노력하였다. 위에서 언급한 내용만 살펴보더라도 일반적인 OS에서 사용하는 보안과는 많은 차이가 있으며, 이를 통해 북한 보안체계의 특수성을 살펴볼 수 있다.

4.2 정책 제언

붉은별 연구를 통해 도출한 시사점을 기반으로 다음과 같은 정책을 제언한다.

첫 번째, 남북협력과 통일에 대비하여 북한 ICT 관련 정보를 지속적으로 수집해야 한다. 국내 국가기관과 여러 협회에서는 남북협력을 위한 다양한 연구를 추진하고 있다. 통일부는

인공지능, 빅데이터 기술을 바탕으로 북한 관련 정보를 분석하는 시스템을 통해 남북협력 및 통일에 대비한 체계적인 북한 종합 지식기반을 구축할 예정이다.[14] 또한 정보통신 단체표준 제정기관인 한국정보통신기술협회(TTA)는 지난 2월, 북한 SW 동향 및 현황조사 연구를 위한 입찰을 공고하였다. TTA는 북한의 SW 동향과 기술현황 관련 정보를 비교, 분석하여 남북 ICT 기술 간의 격차를 파악하고, 향후 남북 ICT 공동 협력을 위한 대안과 기술격차 해소 방안 발굴을 연구 목적으로 설정하였다.[15] 이러한 연구가 내실 있게 추진되기 위해서는 ICT 분야별 북한 현황 파악 및 남북 ICT 용어 비교와 표준화 등이 선행되어야 하며, 북한 SW의 기본정보와 개발 양상에 관한 연구자료는 이러한 국내 연구가 유의미한 결과를 도출하는데 기여할 것이다.

두 번째, 북한이 자체 개발한 다양한 SW에 대한 관심과 연구가 필요하다. 북한은 붉은별 4.0을 기반으로 의학용어를 통일하고 의료 분야 종사자들을 위한 의학용어 보급시스템을 구축하는 등 붉은별 OS를 활발히 활용하고 있다.[16] 또한 북한 중앙과학기술통보사는 기업, 공장과 같은 경제 현장의 경영정보화를 위한 SW 지우 1.0을 개발하여 보급하고 있다. 해당 SW는 경제사업을 당의 의도에 맞게 진행해야 하는 간부들에게 다방면적인 정보를 제공한다.[17] 이처럼 북한은 자체적으로 다양한 SW를 개발하고 있으며, 자체 개발 초기 모델인 붉은별 분석을 토대로 북한 SW 기술 수준에 대한 이해를 넓힐 수 있을 것이다.

세 번째, 북한의 폐쇄성과 특수성을 반영한 SW 보안체계를 이해하고, 우리의 보안체계와 비교 분석하여 보안 대응체계 마련을 위한 연구를 지속해야 한다. 앞서 언급한 붉은별의 보안정책을 통해 북한이 보안에 갖는 관심이 상당하며, 체계적인 보안시스템을 구축하기 위해 노력하고 있음을 알 수 있다. 특히 북한의 선전매체인 조선의오늘은 SW 저작권을 보호할 수 있도록 QR코드 기술이 도입된 SW 제품 보급 및 보호체계 개발사업을 추진하고 있다고 밝혔다.[18] 개발 막바지 단계에 있는 이 시스템이 완성되면 저작권에 대한 불법 침입과 복제 등을 차단하여, 더욱 안전한 정보화 시스템을 구축할 수 있다. 이러한 배경에서 붉은별 운영체제의 문서에 자동생성되는 워터마크 기능에 대한 연구[10]는 북한이 SW 저작권 보호와 보안을 위해 적용한 초기 방식에 대한 분석으로써 북한의 저작권 인식 및 보안 기술 발전 양상에 대한 자료를 제공할 수 있을 것이다.

5. 결론 및 향후연구

본 연구는 북한 OS 붉은별의 특징과 주요 SW, 보안체계를 분석하였으며, 이를 바탕으로 시사점을 도출하고 관련 정책들을 제안하였다.

붉은별의 가장 큰 단점은 외부 인터넷 접속이 불가한 환경이라는 것이다. 이러한 폐쇄성과 특수성으로 인해 붉은별에서는 리눅스의 장점인 오픈소스 기반의 여러 패키지와 SW들을 사용할 수 없고, 이로 인해 국제시장에서 경쟁력을 갖기에는 한계가 있다.

하지만 북한이 SW 산업에 국가 차원의 역량을 집중하고 있다는 점과 북한의 엘리트 교육 및 인적자원의 잠재력을 감안할 때 선진국 기술 수준으로 도약할 가능성을 배제할 수 없다. 특히 북한이 소니해킹, DDoS와 워너크라이 랜섬웨어 공격 등 여러 차례에 걸친 사이버 위협으로 전 세계를 긴장시키고 있는 상황을 고려할 때, 북한 SW 기술과 보안체계 관련 연구가 지속적으로 이뤄져야 한다.

향후 연구에서는 붉은별의 보안성을 기반으로 온톨로지를 설계 및 구현하여, 북한 OS의 세부 기능과 개발 중점, 보안체계의 관계를 분석하고 시각화하기 위한 연구를 진행할 예정이다.

참 고 문 헌

[1] 통일부, “주간 북한동향”, Vol.767, pp.1-39, 2005.

[2] SPRI, “북한 SW 인력과 교육현황” (검색일: 2021.03.13.)

[3] 서울평양뉴스, “北 대학들, 컴퓨터 SW 개발 주력” (검색일: 2021.03.20.)

[4] NK경제, “북한, 시각장애인용 AI 기반 음성인식 낭독기 개발” (검색일: 2021.03.10.)

[5] 김종선, 이춘근, “북한의 컴퓨터 OS 붉은별 분석 및 시사점”, STEPI ISSUES & POLICY, pp.1-16, 2010.

[6] 최성, “북한의 컴퓨터 OS인 붉은별 분석연구”, 한국기술혁신학회 학술대회, pp.230-236, 2011.

[7] 박기훈, 강동수, “북한 OS 붉은별의 보안 취약점 분석”, 한국정보과학회 학술발표논문집, pp.146-148, 2017.

[8] Chanju Park, Dongsu Kang, “A DOM-Based Fuzzing Method for Analyzing Seogwang Document Processing System in North Korea”, KIPS Trans. Comp. and Comm Sys, Vol.8, No.5, pp.119-126, 2019.

[9] 최준형, 강동수, “북한 서광사무처리 3.0 파일 구조 분석”, 한국정보처리학회 춘계 학술대회, pp.335-338, 2019.

[10] 황규섭, 강동수, “붉은별 3.0 Watermarking을 이용한 정보은닉 분석”, 군사과학연구, Vol.13, No.1, pp.1-10, 2020.

[11] 황규섭, 강동수, “북한 OS 붉은별 3.0 침입탐지 규칙 분석”, 한국정보과학회, Vol.27, No.1, pp.48-54, 2021.

[12] 강동수, “북한 소프트웨어와 특허 분석”, 국방대학교 논총, Vol.27, No.2, pp.105-126, 2019.

[13] 김종선, 이춘근, “통일을 대비한 북한의 IT 기술 분석 및 협력방안”, STEPI Insight, (142), pp.1-31, 2014.

[14] 통일부 공식 블로그, “2021 통일부 업무보고”, (검색일: 2021.02.10.)

[15] 한국정보통신기술협회, “북한 SW 동향 및 현황 조사 연구용역” (검색일: 2021.03.23.)

[16] NK경제, “북한, 붉은별 4.0 기반 의학용어 보급시스템 구축” (검색일: 2021.02.12.)

[17] 연합뉴스, “북한, 경제정책에 IT 접목... 간부 경영관리용 프로그램 개발” (검색일: 2021.03.20.)

[18] NK경제, “북한 국가적 SW보급 시스템 구축 마무리 단계“ (검색일: 2021.03.20.)

저 자 소 개

류효진(E-mail: my19910@naver.com)
2014 성신여자대학교 졸업(학사)
현재 국방대학교 컴퓨터공학전공 석사과정
관심분야 : North Korea Software, Ontology

강동수(E-mail: greatkoko@kndu.ac.kr)
2011 고려대학교 컴퓨터공학 박사
현재 국가안보문제연구소 군사과학센터장
현재 국방대학교 컴퓨터공학/사이버전전공 교수
관심분야 : Weapon System Software, North Korea Software, Software Testing, Software Security Testing and Defense Acquisition