Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.6, Dec. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.6.1351

SCADA 디지털포렌식 동향과 향후 연구 제안*

신 지 호,[1†] 서 정 택[2‡]
[1]경찰대학 치안정책연구소, [2]순천향대학교 정보보호학과

Research Trends of SCADA Digital Forensics and Future Research Proposal*

Jiho Shin,[1†] Jungtaek Seo[2‡]
[1]Korean National Police University, [2]SoonChunHyang University

요 약

SCADA가 사이버 위협과 공격에 노출될 경우 사회 곳곳에서 심각한 재해가 발생될 수 있다. 초기의 SCADA 시스템은 설계 시 보안 위협에 대한 고려가 이루어지지 않아 보안 취약성이 높고, 더 큰 문제는 가용성 등의 문제로 즉시성 있는 취약점 패치가 어려운 실정이다. 증가하는 사이버 위협에 신속하게 대응하고 침해사고 예방 및 방지를 위해 SCADA 시스템 보안에 디지털포렌식 절차와 기술이 활용되어야 한다. 본 논문에서는 효과적인 SCADA 포렌식 조사를 위한 연구 방향을 설정하기 위해 SCADA 시스템을 대상으로 디지털포렌식 연구 동향을 살펴보고, 더불어 SCADA 포렌식 대상 및 필요 기술의 분류를 시도하였다. 그 결과, 절차와 방법론에 대해서는 전통적인 디지털포렌식을 크게 벗어나는 연구 결과를 찾지 못했다. 다만, SCADA 시스템만이 가지는 특성을 반영한 접근방법이나 전용 도구를 개발해야 한다는 주장은 의미가 크다. 분석기술에 대해서는 주로 PLC와 전용 네트워크 프로토콜에 대한 취약점 분석에 관한 연구가 주를 이루었다. 이는 SCADA를 대상으로 하는 사이버 위협과 공격이 주로 PLC이거나, 전용 네트워크 프로토콜에 대한 위협이 많았기 때문으로 이해되므로 앞으로도 관련 연구가 지속할 경향으로 보인다. 그러나 조사절차와 분석기법 전반에 걸쳐 SCADA 시스템에서 획득한 증거의 보존이나 무결성과 같은 증거능력에 대한 논의는 거의 이루어지지 않아 아쉬운 부분이다.

ABSTRACT

When SCADA is exposed to cyber threats and attacks, serious disasters can occur throughout society. This is because various security threats have not been considered when building SCADA. The bigger problem is that it is difficult to patch vulnerabilities quickly because of its availability. Digital forensics procedures and techniques need to be used to analyze and investigate vulnerabilities in SCADA systems in order to respond quickly against cyber threats and to prevent incidents. This paper addresses SCADA forensics taxonomy and research trends for effective digital forensics investigation on SCADA system. As a result, we have not been able to find any research that goes far beyond traditional digital forensics on procedures and methodologies. But it is meaningful to develop an approach methodology using the characteristics of the SCADA system, or an exclusive tool for SCADA. Analysis techniques mainly focused on PLC and SCADA network protocol. It is because the cyber threats and attacks targeting SCADA are mostly related to PLC or network protocol. Such research seems to continue in the future. Unfortunately, there is lack of discussion about the 'Evidence Capability' such as the preservation or integrity of the evidence extracting from SCADA system in the past researches.

Keywords: SCADA, ICS, Digital Forensics, SCADA Forensics, Research Trends

Received(09. 19. 2019), Modified(11. 11. 2019), Accepted(12 05. 2019)

* 이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No.NRF-2016M2A8A4952280)과, 2019년도 정부(산업통상자원부)의 재원으로 한국에너지기술평가원의 지원(20162220200010 기후 및 전기환경 변화 적응형 사물인터넷 기반 국가전기안전관리 기술 개발)을 받아 수행된 연구임.

† 주저자, suchme@police.go.kr
‡ 교신저자, soejt@sch.ac.kr(Corresponding author)

I. 서 론

산업 제어 시스템(ICS, Industrial Control System)은 디지털 사회의 핵심이며, 전력 및 수력 발전 제어나 열차 및 지하철 제어 등 우리 사회를 유지하는 핵심 인프라 구성요소이다. SCADA(Supervisory Control and Data Acquisition) 시스템은 자동화된 방식을 이용하여 산업 제어 현장의 기기에서 생산되는 데이터를 실시간으로 수집·모니터링하고 이를 바탕으로 제어하는데 사용된다. SCADA 시스템은 전력·수자원 공급, 석유·가스 분배 시스템을 포함한 많은 중요 인프라가 성공적으로 운영될 수 있도록 기반 아키텍처를 제공하고 있다[1]. 이러한 시스템이 사이버 위협으로 인해 제대로 작동하지 않는다면 전력 공급이 중단되거나, 수량조절에 문제가 생겨 댐이 넘치고, 열차가 충돌하는 등 사회 곳곳에서 심각한 재해가 발생할 수 있다. 그리고 우리는 이미 2010년 Stuxnet의 교훈을 통해 이러한 제어시스템이 오작동할 경우 어떤 결과를 초래하는지 실제 경험을 통해 배운 바 있다.

이처럼 증가하는 제어시스템 대상 사이버 공격에 대한 우려로 SCADA 시스템의 보안성 유지와 취약점 탐지 등 관련 보안 활동이 늘어난 경향이지만, 그 효과는 미미한 편이다. 왜냐하면, 초기 설계 시 보안이 고려되지 않은 제어시스템에 1) 보안성 조치를 하기 위해서는 시스템 자체의 가용성이 현저히 저하되기에 이르고, 2) 폐쇄망에서 이더넷 네트워크로의 전환으로 인해 외부 사이버 공격으로부터 취약성이 증가하였으며, 3) 여러 보안 실증을 위한 테스트베드와 샘플데이터의 부재(不在)로 관련 연구에 곤란함이 존재하기 때문이다. 더불어 제어시스템이 외부의 공격 등으로 인한 사고 발생 시에도 내부기밀유출 등을 이유로 관련 데이터를 공개하지 않아 대응 마련이나 관련 연구에 많은 어려움이 따른다.

그러므로 현재까지 취약점 탐지 위주로 수행되었던 개별 연구 현황에 관한 내용을 분석하고 연구 동향을 종합해볼 필요가 있다. 이에 본 논문에서는 SCADA 시스템에 관한 디지털포렌식 연구 동향을 살펴보고자 한다. 좁은 범위로는 SCADA 시스템의 구성요소에 대한 취약점, 위협탐지와 같은 기술적 대응 측면과 넓게는 SCADA 포렌식 조사를 위한 절차와 가이드라인 등 방법론에 대한 연구 동향을 조사하고자 한다. 이를 바탕으로 SCADA 시스템을 대상으로 하는 향후 디지털포렌식 연구 방향을 제언하고, 더불어 한계점을 도출하고 이를 극복하기 위한 향후 과제 설정도 큰 의미가 있을 것이다.

II. SCADA 시스템 대상 사이버 위협과 디지털포렌식

2.1 SCADA 시스템 대상 사이버 위협

SCADA의 도입 초기에는 시스템을 격리해 독립적으로 운영하였기 때문에 외부의 사이버 공격으로부터 안전하다 여겨졌다. 그러나 SCADA 시스템에 이더넷(ethernet)과 무선통신이 도입된 이후, SCADA는 네트워크를 통한 외부의 사이버 공격에 더는 안전을 보장받지 못했다. SCADA 및 PCS(Process Control System) 시스템은 그동안 공극 전략(Air Gap, Fig. 1.)으로 시스템에 대한 고립화만 추구했을 뿐 보안에 대해서는 오히려 여러 가지 취약한 점이 많았다[2].

외부로부터 물리적으로 격리시켰던 공극 전략은 시스템 인가자가 소유한 USB 저장장치 및 Laptop 컴퓨터를 이용한 감염과 같이, 접근 허용된 사용자를 이용한 '사회공학적 공격'이나, 공개 출처 정보(OSINT)를 활용한 '우회 공격'에 더욱 쉽게 무너졌다. 이런 이유로 공극 구축을 유일한 보안 정책으로

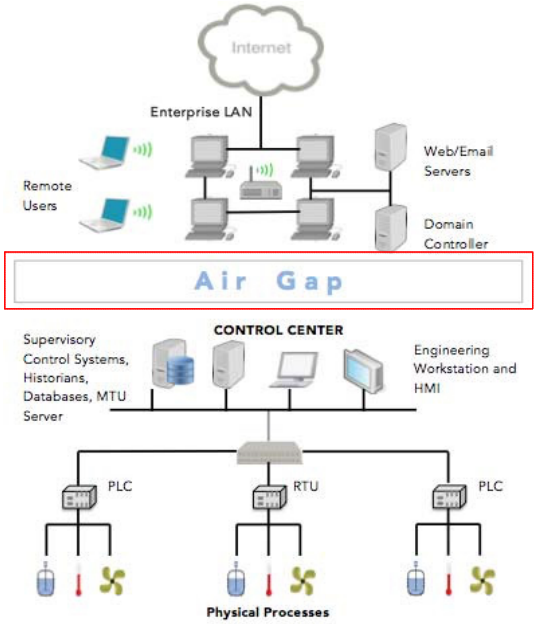


Fig. 1. Conceptual illustration of Air Gap on SCADA(Peter Eden et al., 2015)[3]

활용하던 SCADA는 외부의 사이버 공격으로부터 비교적 정복하기 쉬운 공격 대상이 되었고, 이 같은 피해는 보안 정책과 전략이 설정되지 않은 전통적인 SCADA 시스템에서 발생되었다. 웜(worm)이나 사이버 공격 코드에 쉽게 감염되어 PLC(Programmable Logic Controller)를 비롯한 산업현장의 필드 제어기기가 예기치 않게 오작동 되고, 이는 해당 국가와 사회에 복구 불가한 치명적인 손실을 발생시켰다.

2.2 Digital Forensics

디지털포렌식은 크게 증거의 식별·수집·보존·분석·제출·검증으로 구성되어 있는데(Fig. 2. 참조), 이는 디지털 증거를 확보하기 위한 전체적인 디지털 포렌식 프로세스를 구성하는 메인 프레임이다[4]. '디지털포렌식'이라는 용어를 사용하기 전에는 '컴퓨터 포렌식'이라는 용어를 사용했는데, 발달 초기에 컴퓨터를 대상으로 포렌식 조사와 분석이 주를 이루었기 때문이다. 일반적으로 디지털포렌식은 '디지털 소스로부터 디지털 증거를 보존·수집·증명·식별·분석·해석·기록·제출하기 위하여 과학적으로 이끌어내고 증명하는 방법'으로 정의된다[5].

디지털포렌식은 기술적·절차적으로 동반되어야 할 원칙이 제시되는데, 국내에서는 크게 무결성, 정당성, 절차연속성, 재현성을 기본 원칙으로 다루고 있다[4]. 무결성의 원칙은 디지털 데이터의 본래 특성인 취약성으로부터 비롯된 것으로, 수집한 그 순간에 확보한 디지털 증거가 향후 법정에 제출되기까지 위·변조가 이루어지지 않았다는 성질이다. 정당성의 원칙은 적법절차의 준수와 의미를 같이 하는 것으로, 위법한 방법으로 수집된 디지털 증거는 향후 법적 효력이 상실된다는 성질이다. 절차연속성(chain of custody) 원칙은 무결성의 원칙과 함께 수반되는 원칙으로, Fig. 2.의 전체 디지털포렌식 프로세스에서 부여된 무결성의 원칙이 계속해서 유지된다는 성질이다. 마지막으로 재현성의 원칙은 제3자가 동일한 프로세스를 수행하여 재현할 수 있어야 하며, 법정에 제출된 것과 같은 결론에 도달할 수 있어야 한다는 성질이다. 이 같은 기본 원칙이 유지되는 디지털포렌식을 수행하기 위해서는 디지털포렌식 업무와 관련된 절차와 지침, 규정이 계획되어 있어야 하며, 이를 기반으로 수행되었을 때 그 결과의 객관성을 뒷받침하고 보증할 수 있다.

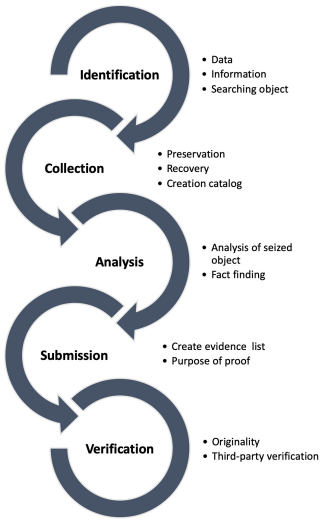


Fig. 2. Traditional Digital Forensics Process (Identification to verification)

이처럼 디지털포렌식은 디지털 데이터를 수집하거나 분석하는데 필요한 '기술'과 그 결과를 합리적으로 증명하기 하기 위해 포렌식 수행 전 주기 동안 따라야 할 '절차'가 융합된 컴퓨터 응용분야라 할 수 있다.

2.3 SCADA에 대한 Digital Forensics 접근

사이버 위협으로부터 SCADA를 보호하기 위해서는 다각적인 대응방안이 필요한데, 먼저 이미 발생된 사이버 공격에 대해서는 사고 대응을 위해 미리 정의된 계획에 의한 세밀한 조사가 필요하다. 즉 사이버 공격 행위에 대한 면밀한 조사를 통해 공격자와 공격 목표, 보안취약점 등 문제점과 피해 규모를 파악하고, 현재 진행 중인 위협을 무력화하거나 최소화하기 위한 대응책을 마련하기 위함이다. 또한, 사이버 공격이 발생하지 않은 상태라 하더라도 보안 정책에 따라 주기적인 예방적 조사를 통해 시스템에 존재하는 취약성을 탐지하고 보완하는 작업을 통해 시스템의 보안성을 높게 유지해야 할 필요가 있다. 즉, 위협 대응과 예방에 디지털포렌식 기술과 절차를 활용할 필요가 있다.

디지털포렌식의 성격으로 비추어보더라도 SCADA 보안 활동에 디지털포렌식 도입이 필요한 이유를 다음과 같이 정리해 볼 수 있다. 먼저, SCADA Forensics은 디지털 매체에서 확보한 증거로부터

특정한 행위의 사실관계를 규명[4]하는 그간의 디지털포렌식 수행 과정과 목적이 유사하거나 일치한다. SCADA 시스템의 구성요소인 PLC, OPC(OLE for Process Control), RTU (Remote Terminal Unit), HMI(Human-Machine Interface) 그리고 필드 디바이스 등은 대부분 마이크로프로세서를 내장한 컴퓨팅 시스템 기반으로 운영되거나 이를 위한 데이터 저장공간이 존재한다(Fig. 3.). 그러므로 이 구성요소 내부의 데이터를 식별-수집-분석하는 과정이 디지털포렌식 절차를 크게 벗어나지 않으므로 조사와 분석에 이를 활용하여 수행되는 것이 좋다.

둘째, 현재 제어시스템에 대한 보안 위협은 대부분 외부의 사이버 공격이 그 원인이 되고 있다. 사고조사를 통해 이를 규명하여 책임을 묻고 때에 따라서는 그 결과에 따른 사실관계를 공히 보증해야 하는데, 이때는 디지털 데이터가 가지는 고유한 물리적·논리적 취약성을 보완할 기술적인 방법을 활용하여

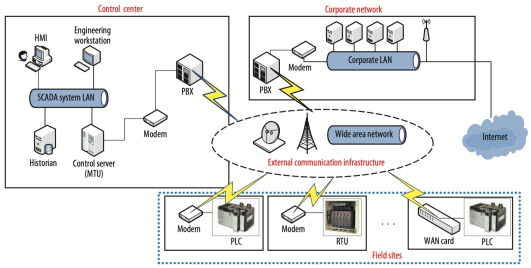


Fig. 3. Simplified logical view of a typical SCADA architecture(Irfan Ahmed et al., 2012)[6]

진정성·무결성·신뢰성·원본성 등이 확보되어야 할 것이다. 디지털포렌식은 이처럼 디지털 데이터의 입증가치를 수집단계에서부터 폐기단계에 이르기까지 신뢰성 있게 유지할 수 있도록 하는 기술적·절차적·법적 요소로 구성된 포괄적인 프로세스[4]이므로 이를 잘 활용해야 한다.

III. SCADA Forensics 기술 및 대상 분류

SCADA 포렌식 수행을 위해서는 먼저 수집과 분석의 대상을 식별해야 한다. SCADA 시스템은 많은 구성요소를 포함하므로 예상되는 대상, 데이터의 상태 그리고 필요한 디지털포렌식 기술을 명확하게 분류해 볼 필요가 있다.

그간의 디지털포렌식은 조사의 대상이 되는 매체를 중심으로 발전되어 왔다. 그러나 디지털 사회에서 사용되는 매체가 다양화되어감에 따라 유체물로서의 디지털기기뿐만 아니라 네트워크 패킷, 컴퓨터 메모리와 같은 디지털 데이터 자체가 디지털포렌식 조사 대상에 포함되었다. 게다가 통신 기술의 발전으로 각종 클라우드 컴퓨팅 및 IoT 기기에서 발생하는 데이터 또한 디지털포렌식의 분석 대상에 포함되었다. 그러나 그간의 디지털포렌식과 같이 SCADA 포렌식 대상을 매체 중심으로 분류를 그대로 따르는 것은 SCADA 시스템 고유의 특성상 무리가 있어 보이므로, 이 논문에서는 Table 1과 같이 SCADA 포렌식의 분류를 크게 '대상'과 '상태'에 따라 분류를 시도하고 다음에서 분류의 정의와 필요성을 기술해 보았다.

Table 1. Taxonomy of SCADA forensics according to traditional digital forensics classification

Category		Target evidence	Target layer (see Fig. 5.)
Object	Disk	Operating system, storage, historian database and internal log	Layer 2, 3, 4, 5
	Memory	Physical memory(RAM)	Layer 0, 2, 3, 4, 5
	Network	Communication packet, connection information, network monitoring, security vulnerability detection	Layer 1, 2, 3, 4, 5
Data Status	Live	Volatile data collection· analysis(such as RAM, network connection information, process information)	All layer
	Silent	Storage and static physical memory(RAM), network packets, malwares, worms	

3.1 대상별 분류

3.1.1 Disk Forensics

디스크 포렌식은 '하드디스크(hard-disk) 포렌식'을 뜻하는 것으로, 컴퓨터 하드디스크의 구조를 분석하고 내부에 존재하던 삭제된 파일을 복구하는 디지털포렌식 초기 발달 분야이다. 현재는 컴퓨터의 주 저장장치가 주로 SSD나 플래시메모리가 이용되어 이에 대한 분석기법이 주로 연구되고 있다. 저장장치의 발달로 외장 저장장치 형태인 USB Stick, CF Card, SD Card 등 플래시메모리를 이용하는 것과 모바일에서 주로 사용되는 NAND 및 eMMC 등도 디스크 포렌식에 포함된다. 이와 같은 이유로 디스크 포렌식보다는 '스토리지(storage) 포렌식'이라는 용어의 표현이 더 적절할 것으로 보인다..

Fig. 1과 3에서 알 수 있듯이 SCADA 시스템의 주요 구성요소들은 마이크로프로세서를 탑재한 컴퓨팅 시스템을 기반으로 운영된다. 또한, 현장 제어 기기의 상태 및 단말 간 통신기록 등 각종 로그의 적재를 위한 전용 데이터베이스를 운영하므로 이를 저장할 공간을 사용하고 있다. 그러므로 디스크 포렌식 기술을 활용하여 이들 저장공간에 대한 포렌식 조사와 분석이 필요하다.

3.1.2 Memory Forensics

메모리 포렌식은 일반적으로 컴퓨터 RAM을 대상으로 디지털포렌식을 수행하는 것을 말한다. 메모리 포렌식은 디지털포렌식의 한 분야로써 뿐 아니라 악성코드 분석, 네트워크 보안, 위협정보수집, 침해사고대응 등 정보보호 분야에서 다양하게 활용되는 응용기술이다. 컴퓨터 메모리는 전원이 인가된 상태에서만 데이터를 획득하고 분석할 수 있으므로 과거의 Live response, Live forensics로 이해되기도 한다.

앞서 논의한 것과 같이 SCADA의 구성요소는 RAM을 이용하는 있는 구성요소가 많다. 예를 들어 PLC는 내부의 사용자 로직을 수행하기 위해 물리 메모리를 사용한다. 4장에서 다시 논의하겠지만, PLC를 대상으로 발생한 외부 공격으로 인해 로직의 변경 여부를 탐지할 때, PLC에 탑재된 메모리의 획득·분석을 통해 데이터의 위·변조를 조사한다. PLC 뿐 아니라 SCADA 최상위 마스터 컴퓨터 및 EWS(Engineering Workstation)나 HMI 등 RAM을 사용하는 구성요소를 대상으로 메모리 포렌식의 수행과 조사가 필요하다.

3.1.3 Network Forensics

네트워크 포렌식은 컴퓨터 네트워크에 관련된 데이터를 수집하고 분석하는 것으로, 주로 네트워크 연결정보나 패킷을 분석하고 모니터링하는 디지털포렌식 활동이다. 패킷은 전송 이후에는 손실되므로 패킷을 효과적으로 획득하는 것이 중요하다. 정상범위를 벗어난 이상 패킷을 모니터링하여 네트워크에서의 이상징후를 탐지하거나, 전송되는 데이터의 보안성을 담보하기 위해 네트워크 구간 암호화 등에 네트워크 포렌식 기술이 이용된다.

SCADA 시스템 또한 이더넷 통신을 기반 네트워크로 사용하므로 각 구간별 패킷 데이터 암호화 등 보안 설정이 필요하다. SCADA에서 주로 사용되는 DNP3, Modbus, PCCC, S7 프로토콜에 관한 연구와 단말-단말 및 중요 통신 구간에 대한 네트워크 퍼징(fuzzing)을 통한 취약구간 식별 등 네트워크 포렌식 기술이 상당히 요구된다.

3.2 상태별 분류

3.2.1 Live Data Forensics

컴퓨터 시스템은 크게 2가지 상태로 나뉘는데, 시스템 전원이 꺼져있는 비활성상태와 반대로 시스템 전원이 켜져 있는 활성상태로 나뉜다. 다시 활성상태에서의 데이터는 휘발성과 비휘발성 데이터로 나뉘는데, RAM과 같이 시스템의 전원차단과 동시에 삭제되는 휘발성 데이터와 로그 파일과 같이 전원차단에 영향을 받지 않는 비휘발성 데이터로 나뉜다. 이를 데이터 측면에서 정리하면, '활성 데이터'는 시스템 전원이 켜있는 상태에서 계속된 데이터의 생성과 사용이 일어나는 휘발성 데이터로, '비활성 데이터'는 시스템이 꺼져있는 상태에서 수집된 데이터나 활성상태 시스템에서 수집된 비휘발성 데이터로 분류해 볼 수 있다.

산업현장의 SCADA는 대부분 시스템이 계속적으로 운영되어야 하는 활성상태 조건이므로, SCADA 포렌식 수행을 위한 데이터 수집에 있어 많은 제약이 따른다. 활성상태 시스템은 비활성상태 시스템보다 상대적으로 데이터의 수집이 자유롭지 못하기 때문에

현장 상황에 맞게 수집이 가능한 데이터 위주의 수집과 조사를 수행해야 한다. IETF RFC 3227 (Guidelines for Evidence Collection and Archiving)[7]나 NIST SP 800-86(Guide to Integrating Forensic Techniques into Incident Response)[8]에서 정의된 휘발성 정도의 기준을 참고하여 수집 순서의 우선순위를 정의하는 것도 좋은 방법이다. 이때 필요한 기술이 라이브 포렌식(live forensics) 기술이다. 활성상태 데이터는 시스템 운영에 따라 의도치 않은 데이터 삭제나 변경이 일어날 수 있으므로 사고 시점으로부터 최대한 빠른 시간 안에 수집하는 것이 중요하다.

라이브 포렌식은 일반적으로 활성 데이터를 대상으로 수행하는 디지털포렌식 활동으로 인식되어있다. 그러나 대용량 저장매체의 보편화로 현장 증거의 복제나 이미징(imaging) 처리에 투입되는 처리시간으로 인한 손실을 줄이기 위해, 즉 사고에 신속히 대응하기 위해 활성상태의 시스템에 존재하는 비활성 데이터의 라이브 포렌식 수행되고 있다[9]. 앞서 논한 대로 SCADA 시스템의 경우 대부분 실제 산업현장에서 운용되고 있는 시스템이므로 침해사고 대응 측면에서 활성 데이터를 다루기 위한 디지털포렌식 기술과 절차를 이용한 대비가 필요하다.

3.2.2 Silent Data Forensics

비활성상태는 시스템의 전원이 차단된 상태를 의미하므로 계속적인 운영 상태를 유지해야 하는 SCADA 시스템의 특성상 활용도가 미미하다 평가 될 수 있다. 그러나 SCADA 시스템에서 수집된 저장장치 및 RAM, 네트워크 패킷의 분석이나 감염된 시스템에서 수집된 악성코드 및 웜의 정적분석 또한 SCADA 포렌식에 있어 매우 중요한 부분을 차지한다.

IV. SCADA Forensics 연구 동향 분석

4장에서는 SCADA를 비롯한 제어시스템 보안 대응 시 디지털포렌식 개념을 접목한 연구 논문 및 문헌을 찾아 동향을 분석하고 시사점을 도출하였다. 관련 연구동향은 크게 SCADA Forensics을 위한 접근방법론, 절차 등을 다루는 Methodology와 분석도구, 분석기법을 다루는 Analysis technique로 나누어 분석했다. 연구동향에 활용될 문헌 검색과 선정을 위해 해외학술정보 사이트 Google Scholar, Research Gate, IEEE Xplore와 국내 학술검색 사이트 DBpia를 이용했다. SCADA에 디지털포렌식 개념을 접목한 문헌이 그리 많지 않은 관계로 SCADA 및 내부 구성요소 키워드를 Digital Forensics 키워드와 조합하여 검색을 실시하였다. 연구 시점과 주제 등을 고려하여 총 10편의 논문 및 문헌을 선별하고 이를 동향 분석에 활용했다(Table 2.).

4.1 SCADA Forensics Methodology

Tina Wu et al.(2013)[10]는 침해사고 발생 후 증거의 훼손을 막고 공격자를 식별하거나 추가 공격을 방어하기 위해 SCADA 시스템에 대한 디지털포렌식 조사절차와 기술이 필요함을 주장했다.

우선 연구자들은 전통적인 디지털포렌식 조사절차를 소개하고 이를 SCADA 시스템에 접목하는 데 한계가 있음을 지적했다. 또한, 그들의 논문에서 Radvanovsky와 Brodsky(2013)가 이미 제안한 'SCADA Digital Forensics Process'를 소개하였는데, 이는 전통적인 디지털포렌식 절차와 크게 다르지 않아 SCADA 시스템에 대한 고려가 충분히 이루어지지 않았다고 지적했다. 그러면서 저자들은

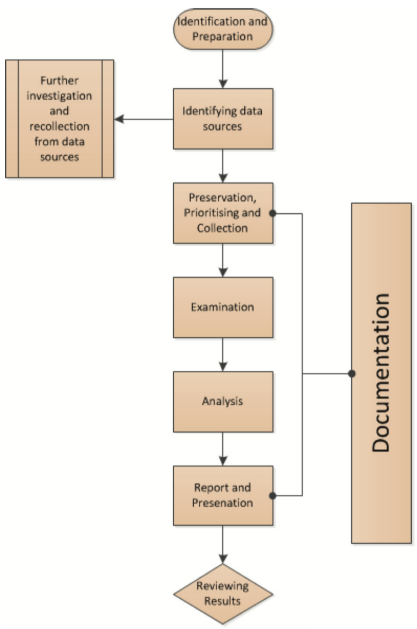


Fig. 4. Forensics process for incident response (Tina Wu et al., 2013)

Table 2. Literature for research trends of SCADA Forensics

	Title / Published	Main Keyword	Author	Year
Methodology	**SCADA Systems : Challenges for Forensic Investigators** *IEEE Computer Society*	Security, Process Control systems, Digital Forensics	Irfan Ahmed et al.	2012
	Towards a SCADA Forensics Architecture *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research*	Digital Forensics, SCADA Forensics, PLC, Process Control	Tina Wu et al.	2013
	Developing cyber forensics for SCADA industrial control systems *The Society of Digital Information and Wireless Communication*	SCADA, ICS, Cyber Forensics, Cyber Security	Joe Stirland et al.	2014
	A Forensic Taxonomy of SCADA Systems and Approach to Incident Response *Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research*	SCADA Forensics, Digital Forensics, ICS Forensics, Critical Infrastructure	Peter Eden et al.	2015
	Guide to Industrial Control Systems Security(NIST 800-82 R2) *National Institute of Standards & Technology*	SCADA, DCS, PLC	Keith Stouffer et.al.	2015
Analysis Technique	**Accurate Modeling of the Siemens S7 SCADA Protocol for Intrusion Detection and Digital Forensics** *Journal of Digital Forensics, Security and Law*	Network, Intrusion-Detection, SCADA, S7	Amit Kleinmann & Avishai Wool	2014
	Exploring The Use Of PLC Debugging Tools For Digital Forensic Investigations On SCADA Systems *Journal of Digital Forensics, Security and Law*	PLC Debugging, Program Code, SCADA, Digital Forensics	Tina Wu & Jason R.C. Nurse	2015
	PLC Forensics Based on Control Program Logic Change Detection *Journal of Digital Forensics, Security and Law*	PLC Forensics, SCADA Security, Ladder Logic Programming	Ken Yau & Kam-Pui Chow	2015
	SCADA network forensics of the PCCC Protocol *Digital Investigation*	SCADA Forensics, SCADA Protocol, PCCC Network Traffic Analysis, PLC	Saranyan Senthivel et al.	2017
	A Forensic Logging System for Siemens Programmable Logic Controllers *IFIP International Conference Digital Forensics*	Programmable Logic Controllers, Forensics, Logging System	Ken Yau et al.	2018

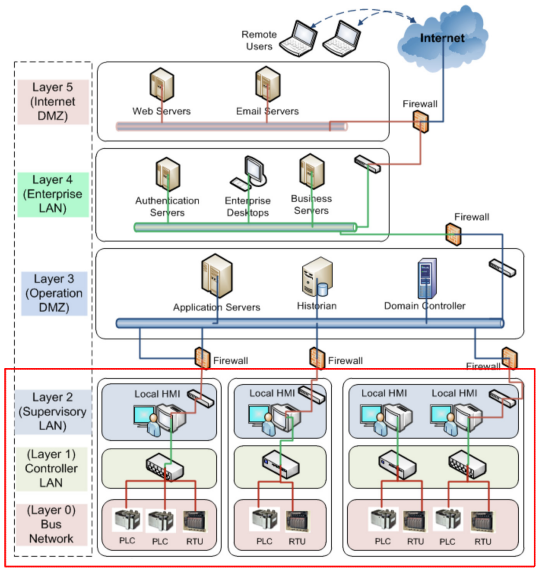


Fig. 5. Layers of SCADA system(Irfan Ahmed et al., 2012)

총 7단계로 이루어진 새로운 SCADA 포렌식 절차를 제안하였으며 각 단계별 수행해야 할 디지털포렌식 활동 내용을 제안했다(Fig. 4.).

이보다 앞서 Irfan Ahmed et al.(2012)[6]은 SCADA 시스템에 대한 포렌식 수사를 위한 조사방법론과 향후 과제를 제시했다. 그는 포렌식 관점에서, 다양한 SCADA 구성요소들 연결성과, SCADA 네트워크와 인터넷과 같은 다른 네트워크와의 연결성을 기준으로 총 6개의 레이어(Layer 0 ~ 5)로 구분하여 접근해야 함을 제안했다(Fig. 5.). Layer 0 - Bus Network는 가장 낮은 단계의 레이어로 Bus network를 통해 연결되어 개별 필드 장치를 포함한다. Layer 1 - Controller Lan은 필드 장치 및 다른 컨트롤러로부터 입력 신호를 수신하는 컨트롤러가 존재하며, 이 컨트롤러는 출력 신호를 전송하여 개별 필드 장치를 조향하는 작업을 수행한다. Layer 2 - Supervisory Lan은 감독 네트워크로, HMI에서 현재 상태를 모니터링 해주는 작업을 위한 하위 계층에 연결된 로컬 네트워크로 구성된다. Layer 3 - Operation DMZ는 Historian, Domain Controller 및 Application Server가 존재하는 DMZ 영역이다. 나머지 상위 계층(Layer 4 ~ 5)은 Enterprise IT Network로, Enterprise Desktop과 Business Server가 운영되는 영역이다. 저자는 이 중에서도 하위 3개 계층(Layer 0 ~ 2)을 디지털포렌식과 가장 연관성이 높고 우선순위를 두어야 할 조사 대상으로 설명했다. 이 계층에 중요한 SCADA 구성요소들이 포함되어있고 Air Gap을 우회한 직접적인 공격이 가능한 대상이기 때문으로 이해된다.

Joe Stirland et al.(2014)[11]은 International Conference of Information Security(InfoSec)에서 SCADA 시스템의 디지털포렌식 절차와 필요한 도구에 관한 연구 내용을 발표했다. 그들은 앞서 발표된 Tina Wu(2013)의 논문과 같이, 기존 전통적인 디지털포렌식 절차의 한계를 지적하며 새로운 절차를 제안했다. 그러나 Tina Wu(2013)가 제안한 SCADA 포렌식 절차[10]와 크게 다르지 않다는 것은 아쉬운 부분이다. 다만, 이 연구에서는 SCADA 포렌식 도구에 대한 논의도 하였는데, 그들이 제안한 절차의 단계별로 활용 가능한 도구를 소개한 것은 큰 의미가 있다. 즉, SCADA 시스템에서 포렌식 조사의 대상 매체를 정리하고, 이를 바탕으로 데이터 수집과 분석에 필요한 도구를 정리하여 제안하였다(Fig. 6. 참조).

Peter Eden et al.(2015)[3]는 앞서 연구자들과 마찬가지로 SCADA 포렌식에 필요한 디지털포렌식 조사 절차론을 제안했다. 그는 SCADA 대상 디지털포렌식 절차를 크게 Prepare, Detect, Triage, Respond와 같이 4가지 영역의 흐름으로 나누었다. Preparation에서는 SCADA 시스템의 구조와 시스템 요구사항 그리고 가능한 공격유형을 준비하는 단계로, Detect에서는 공격의 유형을 정의하고 감염된 구역을 판단하며 격리시키는 단계로, Triage에서는 수집 대상의 데이터를 식별하고 우선순위를 부여하는 단계로, Respond에서는 우선순위가 정해진 데이터를 대상으로 수집, 분석하여 보고서를 작성하는 단계로 설명한다. 이들의 연구가 특별한

SCADA Device:	Phase:	Forensic Tool:
Network	Phase 3.	TCPDump
	Phase 4.	Network Miner, Wireshark, AlienVault
HMI	Phase 3.	Write Blockers, FTK Imager, EnCase, Helix SHA-256/MD5 Hashing Tool
	Phase 4.	EnCase, XWays, Accessdata FTK Toolkit, Volatility
PLC/RTU	Phase 3.	Bespoke PLC Flashing Software
	Phase 4.	XWays
Engineering computer	Phase 3.	Write Blockers, FTK Imager, EnCase, Helix SHA-256/MD5 Hashing Tool
	Phase 4.	EnCase, XWays, Accessdata FTK Toolkit, Volatility
Database Server	Phase 3.	Write Blockers, FTK Imager, EnCase, Helix SHA-256/MD5 Hashing Tool
	Phase 4.	EnCase, XWays, Accessdata FTK Toolkit, Volatility
OPC	Phase 3.	Write Blockers, FTK Imager, EnCase, Helix SHA-256/MD5 Hashing Tool
	Phase 4.	EnCase, XWays, Accessdata FTK Toolkit, Volatility
Historian	Phase 3.	Write Blockers, FTK Imager, EnCase, Helix SHA-256/MD5 Hashing Tool
	Phase 4.	EnCase, XWays, Accessdata FTK Toolkit, Volatility

Fig. 6. Forensic Toolkit Application(Joe Stirland et al., 2014)

점은 Prepare 단계에서 SCADA를 대상으로 발생 가능한 공격유형을 정의하였다는 것이다. 이를 위해 발생 가능 영역을 Hardware, Software, Communication Stack/Protocol로 크게 구분하고, 각 영역별 발생 가능 공격에 대한 유형을 정의했다. 이를테면 Hardware Attack으로는 DOS, Software attack으로는 Buffer Overflow, SQL Injection, Communication Stack/Protocol로는 MITM, Spoofing, Packet Manipulation을 각각 발생 가능한 공격으로 정의하며 상세 공격 방식을 설명했다.

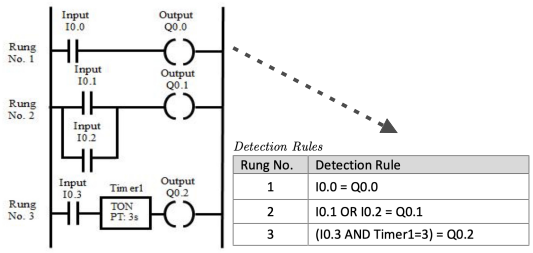
NIST Special Publication 800-82 (Revision2, 2015)[12]는 SCADA/DCS와 같은 제어시스템과 PLC와 같은 구성요소에 대한 보안 가이드라인을 제시한 문서이다. 이 문서는 연구 논문은 아니지만, 산업 제어 시스템을 보호하는 방법에 대한 지침을 제시하며, 시스템의 고유한 성능, 안정성 보장하기 위해 ICS 시스템의 일반적인 위협 및 취약점을 식별하여 관련 위험을 완화하기 위해 권장되는 보안 대책을 제공하므로 SCADA 포렌식 조사절차 및 방법 측면에서 의미가 크다. NIST SP 800-82 내용 중 디지털포렌식 관점에서 눈여겨볼 점은, 제어시스템의 사고 탐지 및 대응 계획, 절차와 방법을 미리 구축해놓아야 한다고 제시하고 있는데, 이는 ①사고를 신속하게 탐지하고 손실과 파괴를 최소화하고, ②추후 포렌식 분석을 위해 증거를 보존하고, ③악용된 약점을 완화하고, ④ICS 서비스를 신속히 복구하기 위해서라고 설명한다. 또, 데이터의 수집과 보존에 대해서도 제시하였는데, 사고 후 적절하고 정확한 데이터 수집이 선행되지 않으면 발생원인 파악이나 추가적인 손상에 대한 대응이 되지 않기 때문에, 이에 관한 계획과 절차를 강조했다.

4.2 SCADA Forensics Analysis Techniques

SCADA의 포렌식 기술에 대한 연구는 주로 PLC와 Network Protocol을 대상으로 많은 연구가 이루어진 경향이다. 즉, PLC와 같은 Device Level과 DNP3, Modbus, PCCC, S7 protocol과 같은 Network Level이 주요 연구 대상이 되었다. PLC는 현장의 센서와 같은 개별 필드장치와 직접적으로 연결되어 있다(Fig. 1, 3.). 상위 계층의 HMI나 제어센터를 공격한 후 이를 이용하여 각 현장의 필드 디바이스를 감염시키는 것은 PLC를 공격하는 것보다 상대적으로 더 많은 시간과 비용이 투자되므로 SCADA 대상 사이버 공격 시 PLC를 직접 공격하는 경우가 많다. 이런 이유로 PLC에 대한 구조와 취약성 분석, 메모리 역분석 등의 관련 연구가 주를 이룬다. 또한, SCADA에서 널리 이용되었던 DNP3, Modbus, PCCC와 Siemens가 제공하는 S7 같은 프로토콜을 이용하여 PLC와 HMI 간 네트워크 통신에 관한 연구 또한 주를 이루었다.

Tina Wu와 Jason R.C. Nurse(2015)[13]는 PLC가 사이버 공격을 받은 경우 PLC에 존재하는 공격용 프로그램 코드가 공격자의 의도를 알 수 있는 중요한 흔적이라 주장하며, 'PLC Debugging Tool'을 이용해서 PLC로부터 프로그램 코드를 획득하기 위한 방법을 제안했다. 그들이 소개한 'PLC Debugging Tool'은 PLC의 메모리 주소에 직접 액세스할 수 있다. 연구자들은 PLC Debugging Tool로는 PLC Logger를 활용하였으며, 벤더가 요구하는 소프트웨어 없이 사용자가 PLC의 메모리 주솟값을 직접 가져올 수 있는 Snapshot 기능은 디지털포렌식 측면의 PLC 메모리 수집 기법으로써 활용도가 높을 것으로 설명했다. 이와 함께 NIST CFTT(Computer Forensic Tool Testing) 프레임워크를 사용하는 포렌식 수집 및 분석 도구로 적합한지를 실험하였으나, 기준에 적합하지 않아 CFTT에서 제시하는 포렌식 도구로서는 한계가 있음을 밝혔다.

Ken Yau와 Kam-Pui Chow(2015)[14]는 PLC 메모리에 적재된 컴파일된 래더(ladder) 로직이 사이버 공격으로 인해 변경되었는지 여부를 탐지하기 위해 그들이 개발한 포렌식 도구 CPLCD(Control Program Logic Change Detection)를 소개하였으며, 실험을 통해 이를 증명했다. Fig. 7과 같이 연구자들은 우선 코드의 변경 탐지를 위해, 사용자의 래더 로직을 Boolean(eg. true or false) 값으로 이루어진 수식으로 변경하는 Detection Rules(DR)을 제안했다. CPLCD는 최초의 정상 DR을 보유한 채로 PLC의 메모리를 실시간으로 탐지하다가, 해당 래더 로직이 미리 정의된 DR과 다르게 실행되는 경우를 외부의 공격에 의해 코드가 변경되었다고 판단하고 이를 탐지하였다. 그러나 CPLCD는 이상 탐지 이후 공격자나 공격 경로 등을 판단하기에는 한계가 존재하며, 이를 위해 와이어샤크(Wireshark)와 같은 네트워크 분석 도구를 추가로 활용할 것을 제안했다.



Detection Rules

Rung No.	Detection Rule
1	I0.0 = Q0.0
2	I0.1 OR I0.2 = Q0.1
3	(I0.3 AND Timer1=3) = Q0.2

Fig. 7. Convert Ladder Logic to Detection Rules(Ken Yau & Kam-Pui Chow, 2015)

Amit Kleinmann와 Avishai Wool(2014)[15]은 Siemens S7 프로토콜에 대한 이상징후 탐지에 관해 연구했다. 이 프로토콜을 사용한 HMI-PLC 간 패킷의 입출력에는 높은 주기성이 있음을 확인하고, 이를 이용한 분석 모델을 개발했다. 즉, 네트워크 패킷의 구조와 종류를 분석하고 비정상 시퀀스(sequence)를 판별하기 위한 모델 DFA (Deterministic Finite-State Automation)를 개발하고, 이를 S7 네트워크 프로토콜의 침입탐지시스템(IDS)에 활용하여 검증했으며 이 모델을 활용한 IDS의 이상탐지율은 99.82%라 밝혔다.

Saranyan Senthivel et al.(2017)[16]은 PCCC 프로토콜을 지원하는 PLC를 이용한 네트워크 포렌식 기법을 제안했다. 연구자들은 실험을 위해 PCCC 프로토콜을 지원하는 Allen Bradley 社(Rockwell Automation의 자회사)의 Micrologix 1400 PLC를 실험에 사용하였으며, 제어 로직 프로그램의 작성과 PLC로의 전송에는 RSLogix 소프트웨어를 활용했다. 이들의 연구가 디지털포렌식 관점에서 큰 의미가 있는 이유는, PCCC 프로토콜에 대해 네트워크 패킷 분석을 시도한 결과 PCCC message field 구조를 파악하였고 더 상세하게는 command & function 코드를 분석하고 네트워크 패킷으로부터 실제 제어 로직을 추출했기 때문이다.

Kam-Pui Chow와 Siu-Ming Yiu[18]은 포렌식 조사를 위한 새로운 PLC Logging 시스템을 제안했다. PLC 감사 로그(audit log)를 저장하는 기존의 도구는 PLC 메모리 변수를 모니터링하고 기록하는 진단(diagnosis)용 도구이므로 포렌식 조사를 위한 충분한 정보가 없어 활용하기에 부적절하다 지적했다. 그들이 제안한 도구는 이러한 한계를 극복하기 위해 Siemens S7 communications protocol 트래픽으로부터 데이터를 추출했다고 설명했다. 이렇게 추출한 데이터는 해석하기 쉬운 포맷의 파일로 작성하여 별도의 전용 저장소에 보관하므로 디지털포렌식 조사를 효과적으로 수행할 것이라고 설명했다.

V. 그간 SCADA Forensics 문제점 및 향후 연구 제안

5.1 그간 SCADA 포렌식의 문제점

4장에서 논의한 SCADA 시스템에 대한 그간의 디지털포렌식 연구 동향과 문제점을 크게 3가지 정도로 도출해볼 수 있다, 첫째, SCADA 포렌식 방법론에 대해서는 대부분 전통적인 디지털포렌식 절차를 이용하여 SCADA의 특징을 다소 반영한 개정 수준으로 제시하고 있어 아쉬운 부분이다. 이 같은 한계는 SCADA 포렌식 조사방법론 개발 시 실제 SCADA 시스템을 직접 활용할 수 없기 때문으로, 이렇게 개발된 조사절차는 전체 SCADA 포렌식 활동 중 일부에만 활용 가능한 단절된 방법론이라 평가할 수 있다. 실무 현장에서 운영되는 실제 시스템을 직접 활용할 수 없다면 테스트베드를 구축하고 이를 활용해야 하는데, 이 또한 쉽지 않다. 개발된 SCADA 시스템의 운영 실증과 보안성 평가, 예방적 대응 등을 위한 테스트베드의 구축에 관한 연구가 긴요하다.

둘째, SCADA 포렌식 기술에 대한 연구 동향은 주로 PLC나 SCADA 네트워크에 관한 연구가 대부분이었다. 이는 SCADA를 대상으로 하는 사이버 위협과 공격이 주로 PLC나 전용 네트워크 프로토콜에 대한 위협이 많았음을 반증한다. PLC는 현장의 센서와 같은 필드 기기와 직접 통신하는 컨트롤러이므로, PLC를 감염시키면 SCADA 관리하는 최상위 제어센터의 감시를 피해 산업현장에 설치된 필드 기기를 멈추거나 오작동시킬 수 있기 때문이다. 그러므로 이들의 보안성을 높이기 위한 계속된 디지털포렌식 연구가 필요하며, 특히 Irfan Ahmed et al.(2012)의 제안과 같이 각 레이어 별 필요한 기술의 연구와 집적이 지속될 필요가 있다. 하지만 PLC, HMI 및 관련 네트워크를 제외한 나머지 분야에 관한 다양한 연구가 미진한 경향이다. 예를 들면, 제어시스템에 대한 외부 공격 발생한 경우 포렌식 조사를 통해 취약점 파악과 공격 범위 등의 판단

을 위해 EWS에 대한 조사가 이루어져야 함에도 이에 관한 연구는 거의 찾아볼 수 없다.

마지막으로, SCADA 포렌식 과정에서 획득된 증거의 '보존'과 '증거능력'에 대한 논의는 거의 찾아볼 수 없다. 앞서 논의한 바와 같이 디지털 증거는 향후 그 증명력을 갖기 위해 공히 인정되어야 하는 "증거능력"을 요하는데, 이는 증거의 올바른 보존을 통한 무결성, 원본성 유지 등 여러 가지 요건으로 완성된다. 그러나 SCADA 시스템에서의 획득하는 증거는 대부분 활성상태 데이터이므로 증거능력을 갖추기에는 그 성질 자체로 부족한 점이 많기 때문에 아예 논의에서 제외되는 것으로 이해된다. 다만, 증거의 보존 측면에서 포렌식 조사에 활용 가능한 메모리 변수나 네트워크 패킷을 전용 저장소에 기록하고 이를 포렌식 조사에 활용해야 한다는 몇몇 연구는 시사하는 바가 크다. 증거능력에 대한 SCADA 시스템 고유의 제약을 극복하기 위해 라이브 포렌식에 관한 연구가 필요하며 이는 향후 과제로 정리할 수 있다.

5.2 한계 및 향후 연구 제안

SCADA 시스템은 PLC, OPC, RTU, Sensor, Actuator 등 전 레이어에 걸쳐 시스템 운영에 필요한 다양한 구성요소들이 포함된 커다란 기반 시스템이다. 그러므로 사이버 공격이나 침해사고가 일어난 공격이 시작된 지점(attack entry point)이나 그 지점과 연결된 구성요소에 대한 감염 여부 등 명확한 디지털포렌식 조사가 이루어질 때 그에 맞는 적합한 대응책을 세울 수 있다. 구성요소에 대한 개별 분석 기술의 경우 관련 연구가 활발하게 진행되고 있지만, 이보다 먼저 통합된 정책을 마련하고 이에 따른 각 레이어별 조사 전략과 분석 방법을 구성하여 체계적으로 수행해야 한다. 그러나 SCADA 시스템에 대한 체계적인 디지털포렌식 조사절차를 사실상 찾기 어렵다.

이와 같은 한계는 첫째, 전통적인 디지털포렌식 조사 방법은 ICS·SCADA 시스템을 포괄하기 어렵기 때문이다. 전통적인 디지털포렌식은 주로 일반적인 IT 인프라 환경에 존재하는 매체를 중심으로 발전되어 왔기 때문에 다양한 구성요소들을 포함하고 있는 SCADA 시스템에서는 활용하기 적절치 않다. 이와 같은 이유로 SCADA 시스템을 조사할 때 그간의 디지털포렌식 조사방법론을 그대로 접목하기에는 무리가 있다. 둘째, ICS·SCADA 대상 디지털포렌식은 대부분 활성상태, 즉 조사 대상 시스템의 전원이 켜져 있고 운영이 유지되어야 하는 가용성 유지 상태에서 데이터 수집이 이루어야 하므로, 데이터를 수집하고 증거를 획득하는데 기술적인 한계가 존재한다. 내부 증거 획득을 위해 SCADA 시스템을 정지한다면 그 손실이 막대하기 때문이다. 이 같은 이유로 전체적인 조사방법론의 연구보다는 SCADA 구성요소에 대한 개별 취약점 탐지 및 디지털포렌식 기법 위주로 연구되는 경향이 있다. 셋째, SCADA에 대한 체계적인 조사절차를 구성하기에는 그간 관련 연구 기간이 다소 짧은 경향이다. 디지털포렌식의 경우, 법과학의 한 분야로 파생된 '컴퓨터 포렌식'을 시작으로 현재까지 40년 이상의 관련 연구와 실무의 역사가 있는 반면, SCADA를 대상으로 증거를 수집하고 분석하는 주된 포렌식 연구는 불과 10년 정도에 이른다. 그나마도 Stuxnet 이전에는 침입 탐지나 IDS 구축 등 주로 취약점 탐지나 관제(monitoring) 위주로 연구되었으므로 체계적인 조사절차를 찾기 힘든 실정이다.

이런 한계를 극복하기 위해 SCADA 시스템에 대한 테스트베드를 구성하고 이를 활용한 디지털포렌식 조사방법론을 적극적으로 개발하여 활용해야 한다. 제어시스템은 안전이나 내부기밀 유지를 이유로 사고 발생 시에도 쉽게 공개되지 않으므로, 위협상황에 대비한 보안 실증을 위한 테스트베드가 필요하다. 하지만 테스트베드 관리에 큰 비용이 투자되고 관련 전문 인력의 지속적인 배치가 어려워 시설의 구축과 연구가 곤란한 상황이다[18]. 테스트베드와 더불어 활성상태의 데이터 획득 및 분석기술, 즉 SCADA 라이브 포렌식 대한 연구 결과의 집적과 SCADA 전용

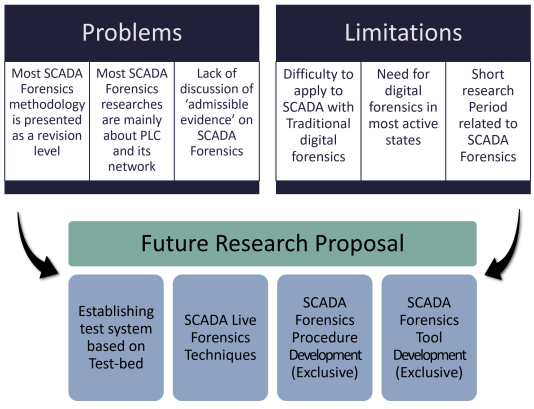


Fig. 8. Problems, Limitation and Future Research Proposal of SCADA Forensics

포렌식 절차 및 도구의 개발도 필요할 것으로 보인다. 이를 도표로 정리하면 Fig. 8과 같다.

5.3 정리

2010년 6월 SCADA를 대상으로 수행된 Stuxnet 공격이 세상에 알려지자, 관련 보안에 관한 관심이 폭증했다. 침입 탐지 위주로 유지되던 관련 연구 또한 다양한 분야로 폭이 넓어졌으며, 산업계는 자신들이 관리·운영하는 제어시스템 전반에 대한 보안 취약성 검증과 보완이 이루어졌다. 그러나 제어시스템을 대상으로 수행되는 공격은 APT(Advanced Persistent Threats) 공격인 경우가 많아 본격적인 제어권 탈취 전까지는 징후나 증상이 없으므로 감염 사실조차도 파악하기 어렵다[12]. 더구나 제어시스템은 계속적인 가용성 유지가 요구되는 핵심 인프라인 경우가 많아 패치 과정에서 의도치 않게 시스템이 오작동 될 부담이 있으므로 취약점을 발견한다 하더라도 즉각적인 대처가 어렵다.

앞서 소개한 연구의 내용을 종합하여 정리해보면, SCADA 시스템의 사고조사와 보안성 유지를 위한 체계적인 'SCADA 포렌식 조사절차와 전용 도구 개발'이 필요하다는 결론에 이른다. SCADA 시스템에 포함된 다양한 구성요소 간 연결성과 외부 네트워크와의 연결 구조 등 SCADA가 가지는 특성을 파악하여 가능한 취약점을 예상하고 사이버 위협에 대응하기 위한, SCADA 시스템에 특화된 디지털포렌식 조사절차와 도구를 마련하는 것이 필요하다.

VI. 결 론

SCADA가 사이버 위협과 공격에 노출될 경우 사회 곳곳에서 심각한 재해가 발생할 수 있다. 초기의 SCADA 시스템 설계 시 보안 위협에 대한 고려가 이루어지지 않았고, 더 큰 문제는 가용성 등의 문제로 즉시성 있는 취약점 패치가 어려운 실정이다. 증가하는 사이버 위협에 신속하게 대응하고 침해사고 예방 및 방지를 위해 SCADA 시스템 보안에 디지털포렌식 절차와 기술이 활용되어야 한다. 본 논문에서는 효과적인 SCADA 포렌식 조사를 위한 향후 연구 방향의 설정을 위해 그간의 SCADA 포렌식 연구 동향을 살펴보고 SCADA 포렌식 분류를 시도해 보았다. 그 결과, 절차와 방법론에 대해서는 전통적인 디지털포렌식을 크게 벗어나는 연구 결과를 찾지 못했다. 다만, SCADA 시스템만이 가지는 특성을 반영한 접근방법이나 전용 도구를 개발해야 한다는 주장은 의미가 크다. 분석기술에 대해서는 주로 PLC와 전용 네트워크 프로토콜에 대한 분석기법이 주를 이루었다. 이는 SCADA를 대상으로 하는 사이버 위협과 공격이 주로 PLC나 전용 네트워크 프로토콜에 대한 위협이 많았기 때문으로 이해되므로 앞으로도 관련 연구가 지속할 경향으로 보인다. 그러나 조사절차와 분석기법 전반에 걸쳐 SCADA 시스템에서 획득한 증거의 보존이나 무결성과 같은 '증거능력'에 대한 논의는 거의 이루어지지 않아 아쉬운 부분이다.

향후에는 지금까지의 연구 동향을 기초로 이미 구축된 발전시스템과 그로부터 생성된 에너지의 수송과 공급, 그리고 교통 운송 등 국내 사정의 SCADA 시스템의 특성 및 구조를 면밀히 파악하고 이에 적합한 디지털포렌식 조사방법론과 분석기술 연구, 더불어 SCADA에서 획득한 증거의 보존과 증거능력에 관한 연구가 후속되기를 기대한다.

References

[1] Tina Wu & Jason RC Nurse, "Exploring the use of PLC debugging tools for digital forensic investigations on SCADA systems," Journal of Digital Forensics, Security and Law, vol 10, no.4, pp. 79-96, 2015

[2] Hyung-Geun Park, "Detailed Analysis Report of Stuxnet," IBM Security, IBM Korea, 2010

[3] Peter Eden et al. "A forensic taxonomy of SCADA systems and approach to incident response," Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research. BCS Learning & Development Ltd., pp. 42-51, 2015

[4] Hee-Sung Tak and Won-Sang Lee, "A Study on a Model Frame for the Integration of Digital Forensic Processes," Research Series 16-AA-01, Korean Institute of Criminology, 2017

[5] DFRWS, “A Road Map for Digital Forensics Research”, DFRWS Technical Report, DFRWS, 2001
[6] Irfan Ahmed et al. ″Scada systems: Challenges for forensic investigators,″ Computer, vol. 45 no. 12, pp. 44-51, 2012
[7] Dominique Brezinski et al., “Guidelines for Evidence Collection and Archiving”, RFC 3227, International Engineering Task Force, 2002
[8] Karen Kent et al., “Guide to Integrating Forensic Techniques into Incident Response”, Special Publication 800-86 , National Institute of Standards and Technology, 2006
[9] Forensic Proof, “Live Forensics”, http://forensic-proof.com/archives/3378
[10] Tina Wu et al., ″Towards a SCADA forensics architecture,″ Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research, vol. 12, pp. 12-21, 2013
[11] Joe Stirland et al. ″Developing cyber forensics for SCADA industrial control systems,″ The International Conference on Information Security and Cyber Forensics (InfoSec2014), The Society of Digital Information and Wireless Communication, pp. 98-111, 2014
[12] Keith Stouffer et al., “Guide to Industrial Control Systems(ICS) Security”, Special Publication 800-82 Rev.2, National Institute of Standards and Technology, 2015
[13] Tina Wu and Jason R.C. Nurse, ″Exploring The Use Of PLC Debugging Tools For Digital Forensic Investigations On SCADA Systems,″ Journal of Digital Forensics, Security and Law, vol. 10, no. 4, pp. 79-96, 2015
[14] Ken Yau and Kam-Pui Chow, ″PLC Forensics Based on Control Program Logic Change Detection,″ Journal of Digital Forensics, Security and Law, vol. 10, no. 4, pp. 59-68, 2015
[15] Amit Kleinmann and Wool, Avishai, ″Accurate Modeling of the Siemens S7 SCADA Protocol for Intrusion Detection and Digital Forensics,″ Journal of Digital Forensics, Security and Law, vol. 9, no. 2, pp. 37-50, 2014
[16] Saranyan Senthivel et al., ″SCADA network forensics of the PCCC protocol,″ Digital Investigation, pp. 57-65, 2017
[17] Ken Yau et al., “A Forensic Logging System for Siemens Programmable Logic Controllers,” IFIP International Conference Digital Forensics : Chapter 18, pp. 331 - 349, 2018
[18] Hyung Cheon Kim, “ICS Dataset for Security Research”, 4th CPS Security Workshop, KIISC, pp. 23-37, 2019

〈저자소개〉

신 지 호 (Jiho Shin) 정회원
2015년 2월: 고려대학교 정보보호대학원 디지털포렌식학과 석사
2019년 3월~현재: 순천향대학교 정보보호학과 박사과정
2008년 7월~2011년 1월: 경기시흥경찰서 사이버범죄수사팀 수사관
2011년 7월~2015년 1월: 경기남부지방경찰청 디지털포렌식계 분석관
2015년 1월~2018년 1월: 경찰대학 국제사이버범죄연구센터 선임연구원
2018년 1월~현재: 경찰대학 치안정책연구소 과학기술연구부 연구관
〈관심분야〉 디지털포렌식, 제어시스템 보안, 사이버범죄

서 정 택 (Jungtaek Seo) 종신회원
1999년 2월: 한국교통대학교 컴퓨터공학과 학사
2001년 2월: 아주대학교 컴퓨터공학과 석사
2006년 2월: 고려대학교 정보보호공학과 박사
2000년 11월~2016년 2월: 국가보안기술연구소 책임연구원/연구부장
2014년 6월~2015년 6월: University of Florida 초빙연구원
2016년 3월~현재: 순천향대학교 정보보호학과 조교수
2009년 12월~2013년 5월: 제주 수마트그리드 실증단지 보안센터 센터장
2013년, 2018년: 한국철도공사 정보화자문단 자문위원
2016년 1월~2016년 12월: ㈜ SR 철도안전자문단 자문위원
2017년 1월~현재: 한국정보보호학회 CPS보안연구회 회장
2017년 2월~현재: 한국남동발전 사이버보안자문단 자문위원
2017년 11월~현재: 인천국제공항공사 사이버보안 자문위원회 위원
2018년 12월~현재: 한국서부발전 사이버보안 자문위원
〈관심분야〉 CPS보안, 제어시스템 보안, 스마트그리드 보안, 원자력 발전 사이버보안, 스마트시티 보안, 스마트팩토리 보안 등