2020 소프트웨어공학종합프로젝트(캡스톤디자인) 최종 발표

스마트미터(AMI) 공격 시나리오 기반 인공지능 NIDS 개발

캡스톤디자인 A2조 | 145204 윤성수
160542 신미주
175650 임수민

목차

주제 선정

Topic selection

1. 배경

» 스마트미터 관련 동향


지식경제부 공고 제2012-365호

『지능형전력망의 구축 및 이용촉진에 관한 법률』 제5조(지능형전력망 기본계획의 수립·시행), 제6조(지능형전력망 시행계획의 수립·시행)에 따라 수립된 제1차 지능형전력망 기본계획 및 2012년도 지능형전력망 시행계획을 동법 시행령 제2조 및 제4조에 따라 다음과 같이 공고합니다.

2012년 7월 20일
지식경제부장관

제1차 지능형전력망 기본계획

2012. 7. 20.

관계부처 합동

제1차 지능형전력망 기본계획 주요내용

세계최초 7大 광역권별 거점도시 구축
스마트그리드 거점도시

소비자 / 신규서비스 사업자

전기자동차 / 신재생 에너지 보급확산과 연계

시장창출 > 신규서비스출현 > 제도개선


제2차 지능형전력망 기본계획
(2018~2022)

2018. 8.

산업통상자원부

정책 과제

1 스마트그리드 新서비스 활성화	2 스마트그리드 체험단지 조성
계절별·시간대별 요금제 확대	스마트그리드 서비스 체험단지 조성
국민 DR로 확대 개편	4 스마트그리드 확산 기반 구축
전력 빅데이터 기반 新사업모델 창출	민관 정책 협력 네트워크 강화
전력중개사업 도입·시행	5대 부문별 기술개발·표준화
3 스마트그리드 인프라·설비 확충	상호운용·표준기반 확충
AMI 인프라 확충	산업진흥 및 수출산업화 지원
실시간 기반 전력망 운영체계 구축	소비자 권리·개인정보 보호 강화
전력망의 ICT 인프라 확충	융합형 혁신인력 양성

지능형전력망의 구축 및 이용촉진에 관한 법률 (약칭: 지능형전력망법)

[시행 2017. 9. 22.] [법률 제14674호, 2017. 3. 21., 일부개정]

산업통상자원부(전력진흥과), 044-203-5266

지능형전력망의 구축 및 이용촉진에 관한 법률 시행령 (약칭: 지능형전력망법 시행령)

[시행 2020. 3. 3.] [대통령령 제30509호, 2020. 3. 3., 타법개정]

산업통상자원부(전력진흥과), 044-203-5266
산업통상자원부(분산에너지과), 044-203-5194

한전 HPGP AMI 사업 추진 여부에 촉각

스마트미터링처, HPGP PLC형 AMI 테스트 통과업체 12개사 소집

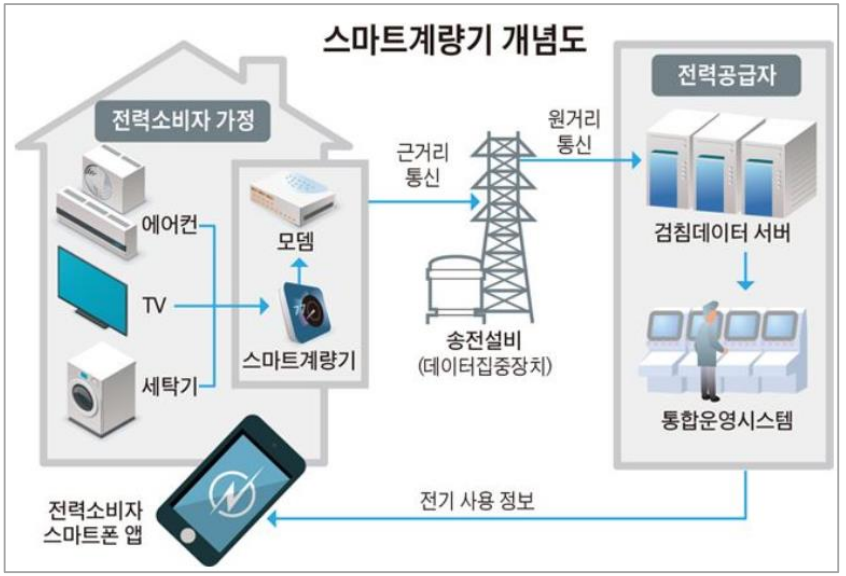
입찰 및 보안모듈 문제 등 논의, 한전, "늦어도 4월 중 공고 예정"

강수진 기자 작성 : 2020년 03월 09일(월) 11:44 게시 : 2020년 03월 09일(월) 17:01

» 최근 **국내에서 AMI(스마트 미터) 도입을 추진** 중에 있음

1. 배경

›› AMI 란?



- 지능형 원격 검침 장치, 스마트 전력량계
- 스마트 그리드의 핵심 요소
- 전기 사용량과 시간대별 요금 정보 등의 데이터를 수집하여 실시간으로 소비자와 공급자 양방향에 제공

1. 배경

›› 스마트 미터 공격 사례

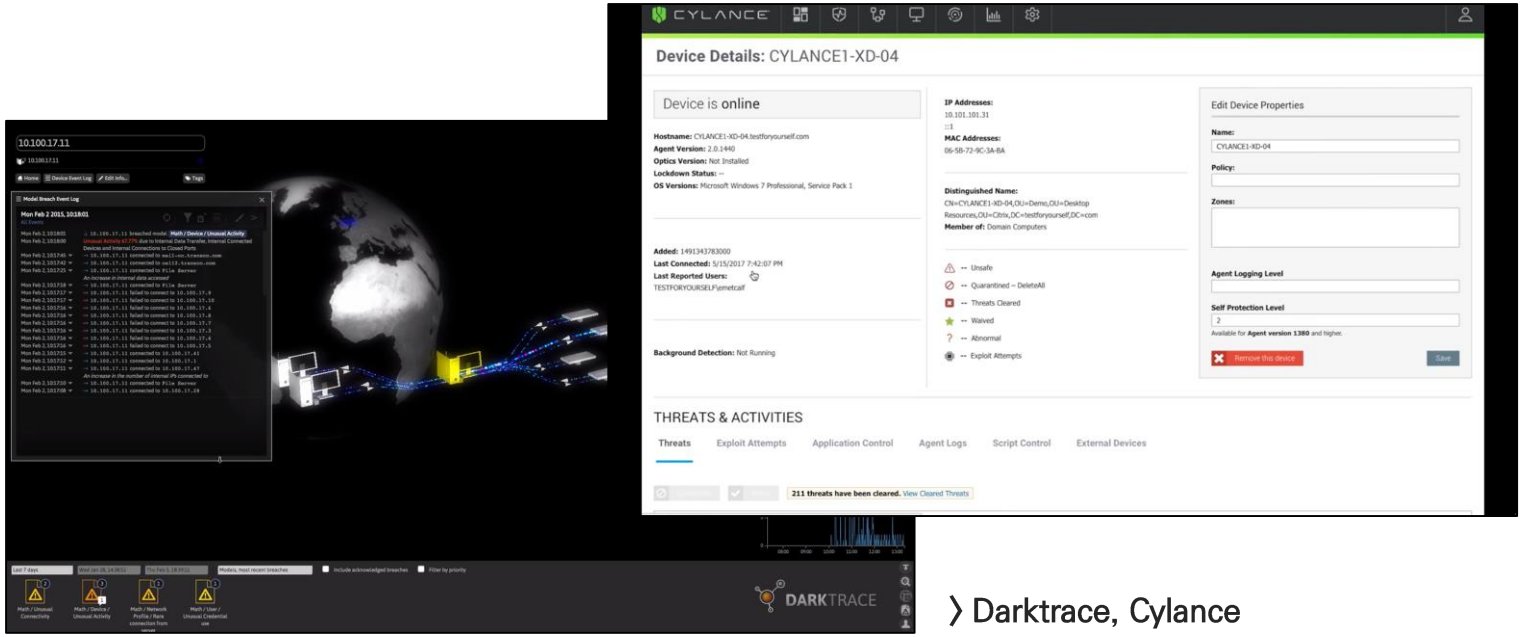
- 스마트 미터 해킹을 통해 운영 센터가 침입된 사건
- 스마트 미터 취약점을 공격하는 **웜 전파 시뮬레이션**이 BlackHat에 의해 이루어졌으며 **24시간에 25,000대의 스마트 미터를 감염**시킴
- **DDoS 공격을 통해 스마트미터가 마비**되는 것을 보였으며, 스마트미터 취약점을 이용 하여 웜을 감염시키고 주변으로 전파하는 것을 시연.

(출처, AMI treats, intrusion detection requriements and deployment recommendations IEEE,2012)

›› AMI(스마트 미터) 도입 시 **해킹 위협 발생 가능**

1. 배경

» IDS/IPS 솔루션 동향



〉Darktrace, Cylance

» 최근 판매되는 IDS & IPS에 **머신러닝, 딥러닝 기술**이 주로 적용됨

“스마트 미터(AMI) 공격 시나리오 기반 인공지능 NIDS 개발 ”

2. 주제 선정

›› 탐지 공격 타켓팅 & 탐지 모델 선정

- 탐지 공격 유형 : DoS/DDoS
- 학습 및 검증 데이터셋 : CICIDS2017
- 탐지 모델 : Auto Encoder

2. 주제 선정

›› 공격 유형, 왜 DoS, DDoS 인가?

- (2019) Exploring Severity Ranking of Cyber-Attacks in Modern Power Grid

Type of Attack	Voltage Index at PCC		
	With Attack	Without Attack	Severity Ranking
DDoS	0.4029		1
FDI	0.1338	0.0435	4
Compromised Key	0.1156		5
Man-In-Middle	0.08147		8
Replay	0.0815		7
Crash Override	0.2095		3
Packet Drop	0.0665		9
Jamming	0.4028		2
Stealthy Deception	0.1089		6

›› 전력 망에서 공격 수행 시 **가장 큰 파급 효과를 보이는 공격**

2. 주제 선정

›› 데이터 셋, 왜 CICIDS2017인가?

데이터 셋	정상 (비율)	DoS/DDoS (비율)	총 데이터	최신 공격 기법 반영
ISCX-IDS-2012	739,300 (94%)	41,236 (5%)	780,536	X
KDDCup-99	157,870 (20%)	621,311 (79%)	779,181	X
KISA 정보보호 R&D	2,883,653 (99%)	129 (0.00004%)	2,883,782	O
CICIDS-2017	440,032 (63%)	251,723 (37%)	691,755	O

- CICIDS-2017은 총 691,755개 중 정상 데이터 440,032개, 공격 데이터 251,723개로 다른 오픈 DOS/DDOS 데이터 셋에 비해 **데이터 불균형이 적었음**

2. 주제 선정

›› 탐지 모델, 왜 AutoEncoder 인가?

1. 머신러닝 / 딥러닝을 이용한 이유
   최신 **공격의 패턴을 학습**하여 IDS에 즉시 적용할 수 있는 방법이 필요.

2. 비지도 학습을 이용한 이유
   비지도 **학습은 특징 간의 관계성을 스스로 학습 및 예측**하기 때문에 지도 학습의 한계를 극복할 수 있다고 판단

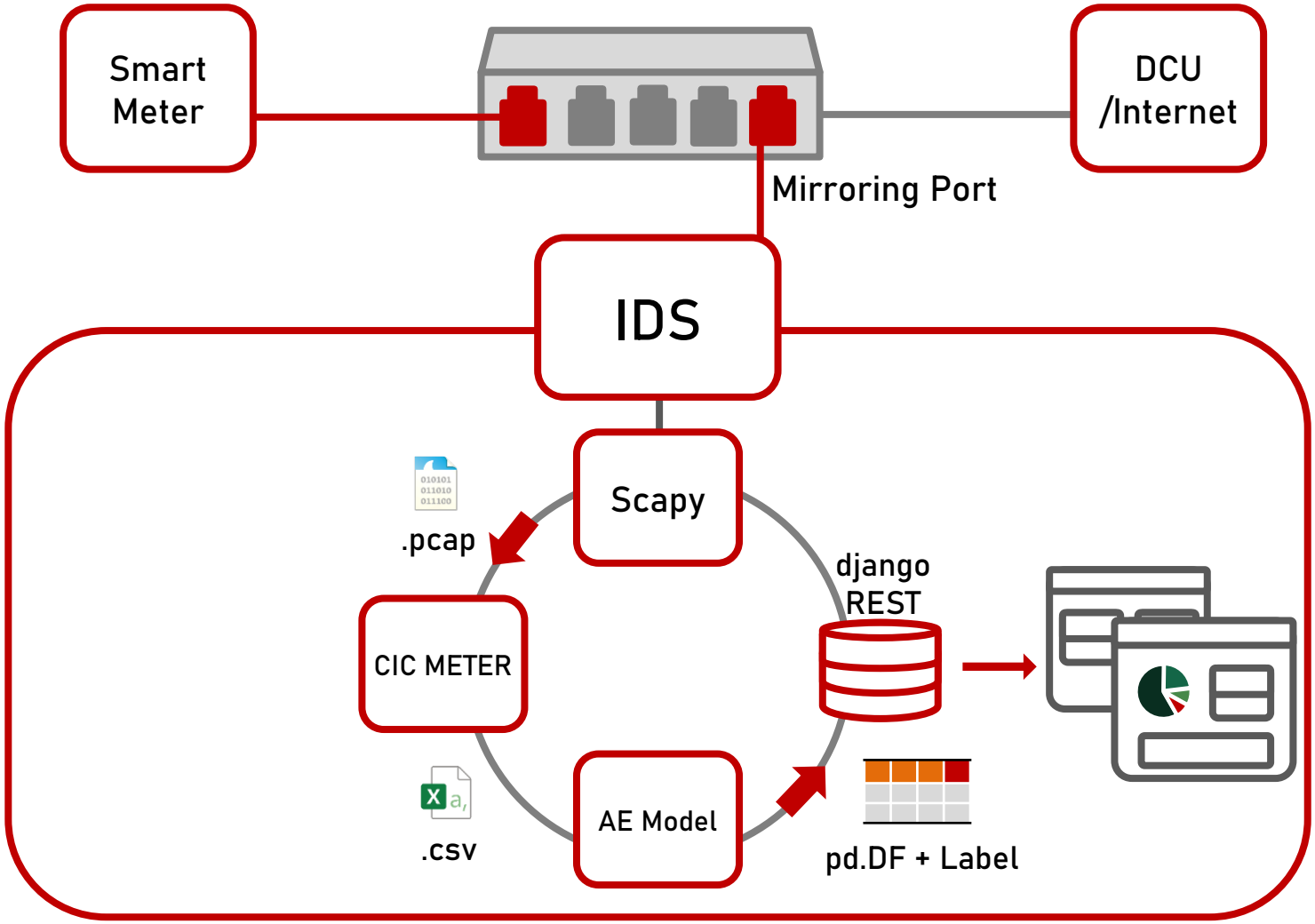
3. AutoEncoder를 사용한 이유

학습 방법	알고리즘	Precision	Recall	Accuracy
지도 학습	KNN	0.99	0.83	0.94
	Decision Tree	0.98	0.89	0.95
	Random Forest	0.99	0.89	0.96
	SVM	0.97	0.63	0.86
	DNN	0.92	0.92	0.94
비지도 학습	Kmeans-Clustering	0.97	0.52	0.82
	Auto Encoder	0.95	0.95	0.93

- 학습한 비지도 학습 알고리즘과 지도 학습 알고리즘과 비교했을 때, **AutoEncoder가 공격 데이터 탐지에 있어서 전체적으로 성능이 더 좋다고 판단**

아키텍처
Architecture

3. 아키텍처


Smart Meter
DCU /Internet
Mirroring Port
IDS
Scapy
.pcap
CIC METER
.csv
AE Model
django REST
pd.DF + Label

AMI_IDS

Current Attack Log

11	[공격탐지] (192.168.0.87:54168) > (35.224.99.156:54168) TCP
15	[공격탐지] (192.168.0.13:4525) > (192.168.0.122:4525) TCP
23	[공격탐지] (192.168.0.13:4523) > (192.168.0.122:4523) TCP
41	[공격탐지] (192.168.0.13:4525) > (192.168.0.122:4525) TCP
43	[공격탐지] (192.168.0.13:4522) > (192.168.0.122:4522) TCP

Attack Counts

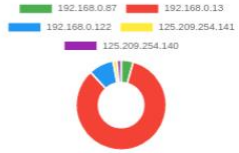
최근 10분간

1249 건의

DDoS 공격이 발생하였습니다.

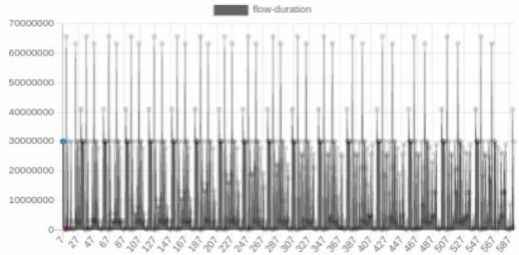
Top5 Protocol

Top5 Src-ip

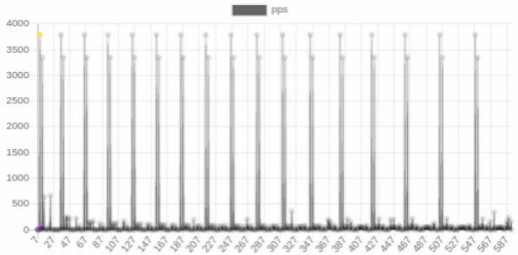


Top5 Src-port

Flow duration Graph



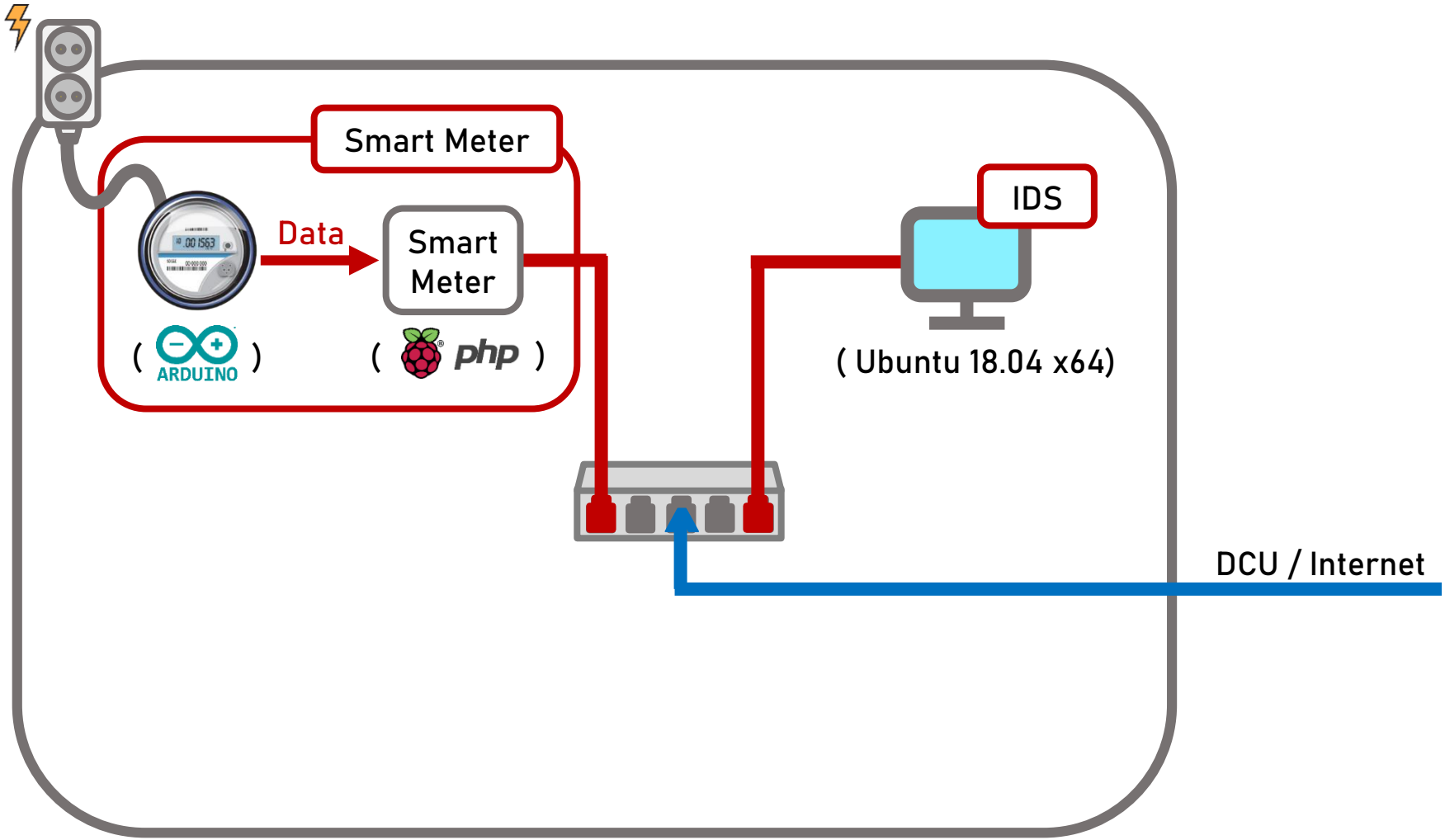
PPS duration Graph



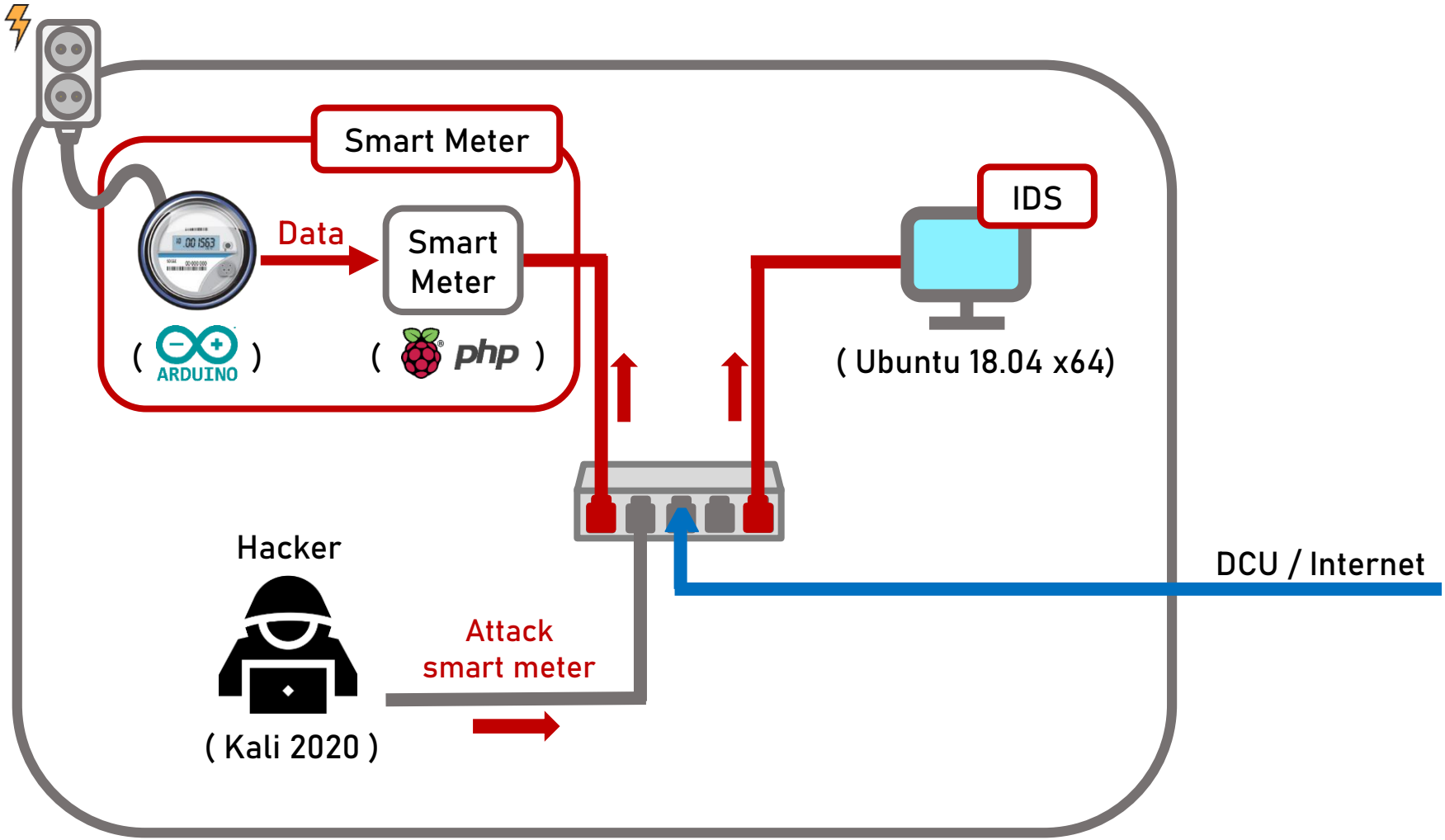
공격 시나리오

scenario

4. IDS 배치


Smart Meter
Data
Smart
Meter
(ARDUINO)
(php)
IDS
(Ubuntu 18.04 x64)
DCU / Internet

5. 공격 시나리오



› **가정** : 공격자는 내부 네트워크를 침입하여 공격을 수행함

시연 영상
Presentation


스마트 미터와 네트워크 TAP 장비

요약

1. 최근 국내 AMI 도입 추진 중. 스마트미터 도입으로 야기될 수 있는 위협에 대응하기 위해서 AMI 환경 기반 IDS 의 필요성이 대두됨

2. 다양한 인공지능 모델을 비교 분석하여, 최적의 모델을 적용시킨 인공지능 IDS 개발

3. 실제 간이의 AMI환경과 공격 시나리오를 구축하여, 개발한 IDS의 정상적인 동작 확인

감사합니다.

캡스톤디자인 A2조 | 145204 윤성수
160542 신미주
175650 임수민