경제 3혁신 3개년 계획
3년의 혁신, 30년의 성장

Creative Economy 창조경제

K-ICT International Conference on Information Security (ICIS) 2015

IoT Cyber Incidents trend and Countermeasures

Son kijong(KISA)

미래창조과학부 Ministry of Science, ICT and Future Planning

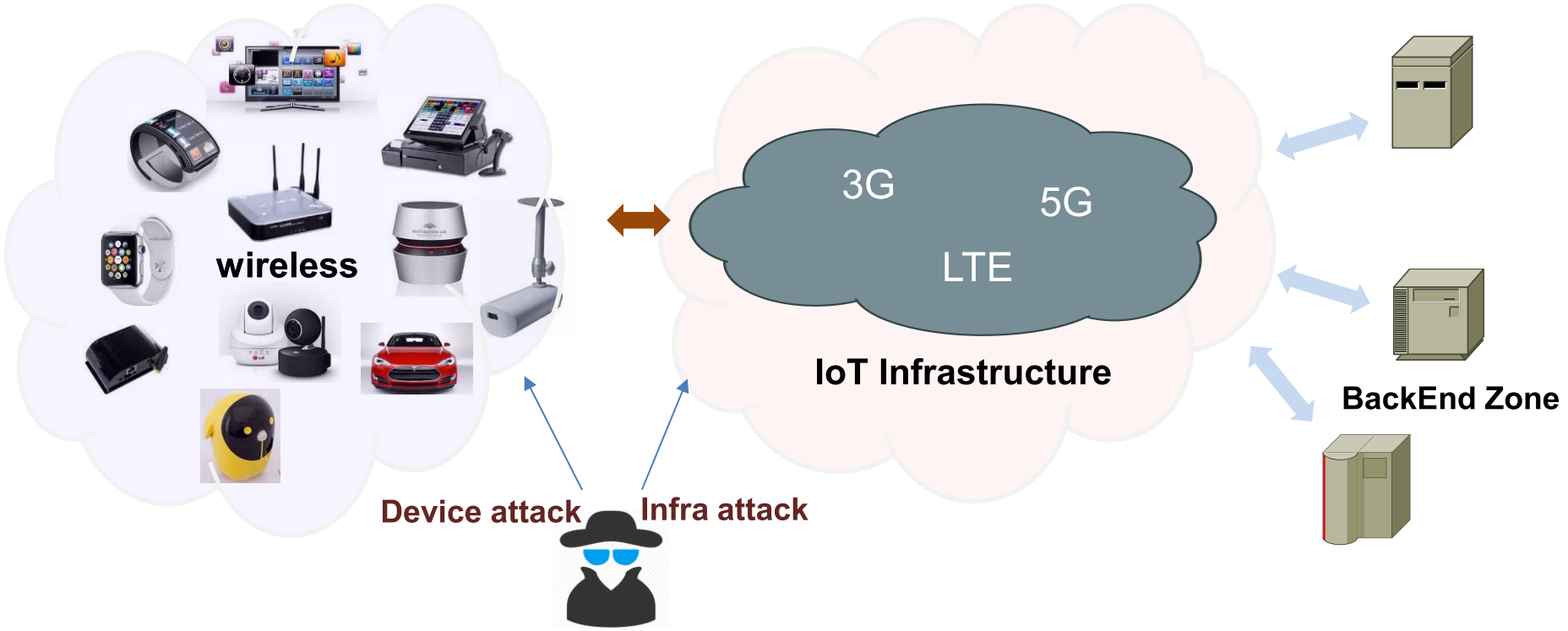
KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

1. IoT security threat
2. IoT cyber attack trends
3. Countermeasures

1. IoT security threat

- The attack target in IoT service environment

- IoT devices and Service Infrastructure

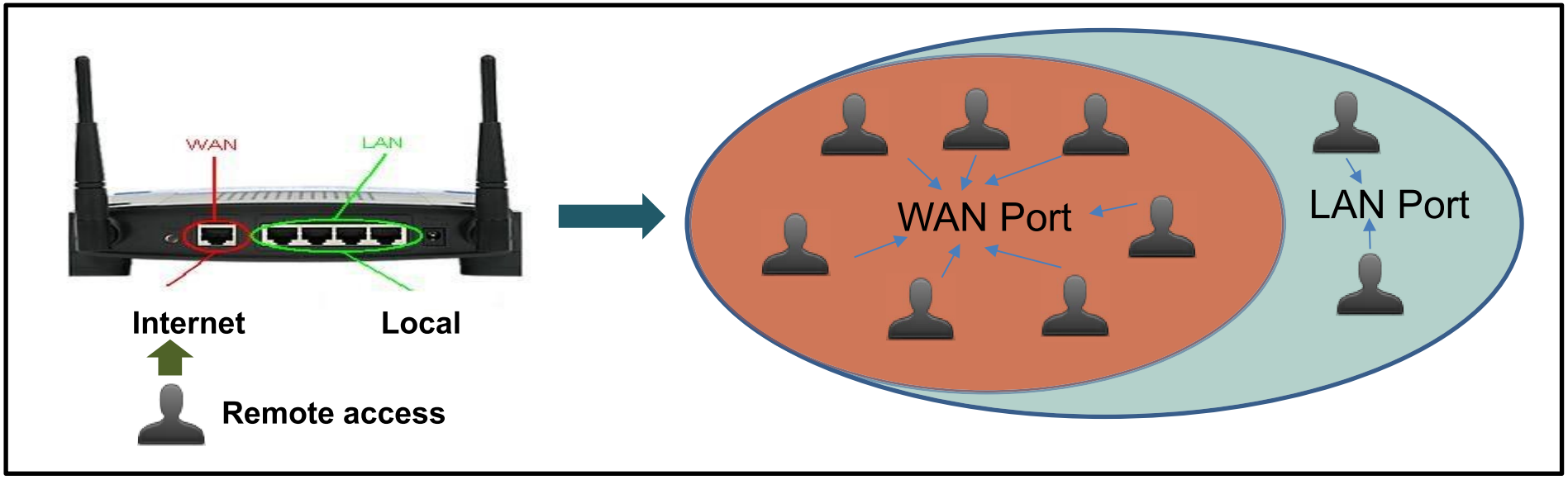


1. IoT security threat

- Security issues from the external communication

- Remotely access of multiple IoT devices

- Compromised IoT devices by exploiting to the vulnerable services



1. IoT security threat

- Secret remote administration function in IoT devices
  - Attack and exploit remote admin tool of IoT Manufacturers
  - Extracting hidden remote access password in Firmware file
  - Firmware update to remove this secret admin tool

FIRMWARE dumping

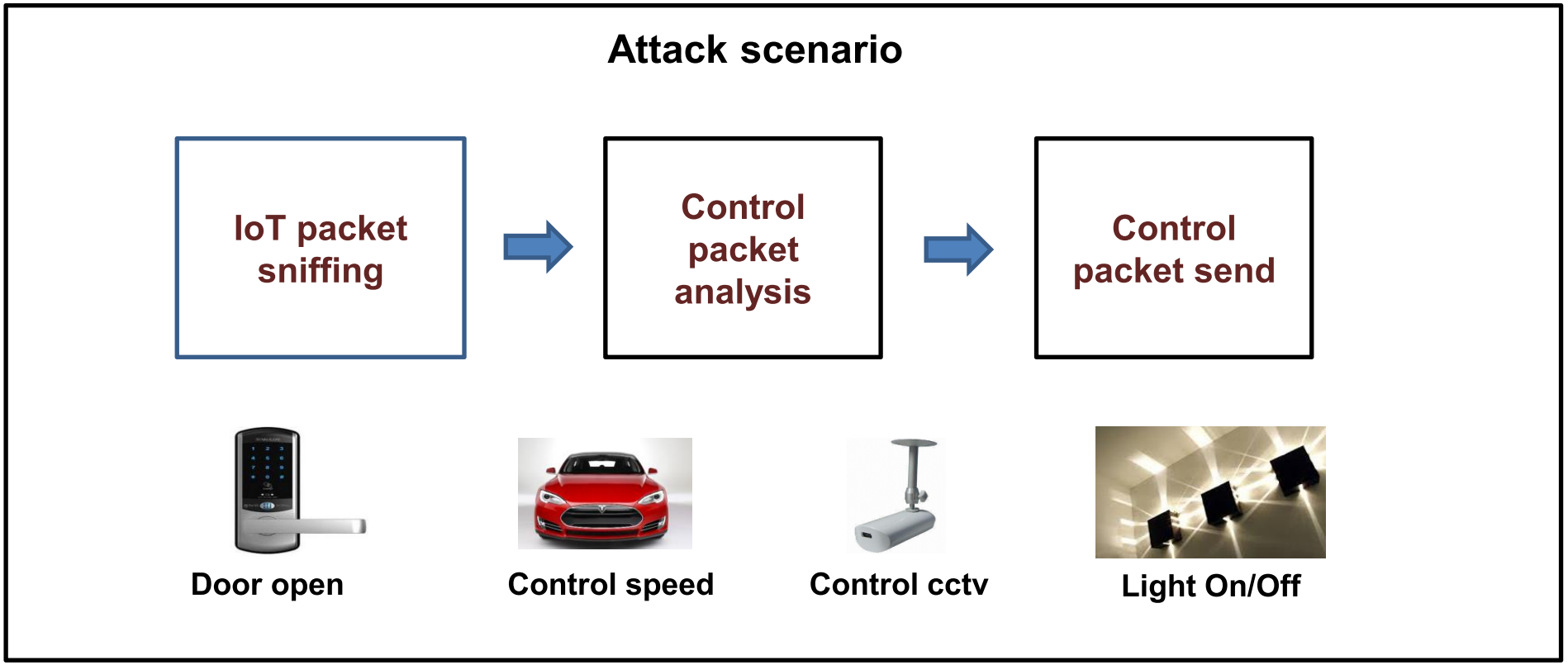
UART
Interface

Hidden remote access password

1. IoT security threat

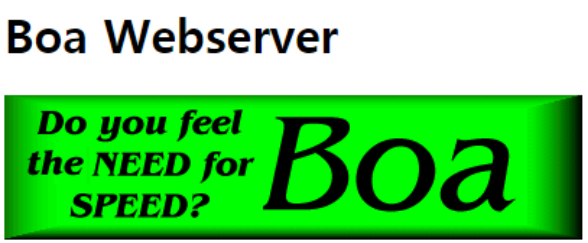
IoT devices remote control and malfunction threat

- Remote control using packet replay attack



1. IoT security threat

- Open source software vulnerabilities



GHOST vulnerability

1. IoT security threat

- Attack IoT service systems and infrastructure

  - Attack enterprise networks via IoT devices of customer

  - Attack internal server connected IoT devices of employee

  - Hacking IoT systems using network packet manipulation

  - Privacy issue of cloud server

1. IoT security threat

▶ Security issue related to user

- Lack of security awareness ▶old firmware version, etc

- Continual exposure under attack caused by low patch

- Not installed security alert program in IoT devices

- Lack of update method about discontinued Model

- Firmware update environment

2. IoT cyber attack trend

▶ PRIVACY ISSUE

Privacy life disclosure

A user card information
CardID: 1002-010-102
Name : Hong
Tel : 010-1111-2222
Date: 17-02-11
B user card information
…..

Privacy data disclosure

2. IoT cyber attack trend

- Increasing DDoS/DRDoS attack

- SSDP Reflection attack

2. IoT cyber attack trend

▶ Increasing DDoS/DRDoS attack

- SSDP Reflection attack

1. Use udp packet(1900 port)

2. Spoofed source ip address == victim address

3. Attack target ▶ devices enabled remote access UPnP

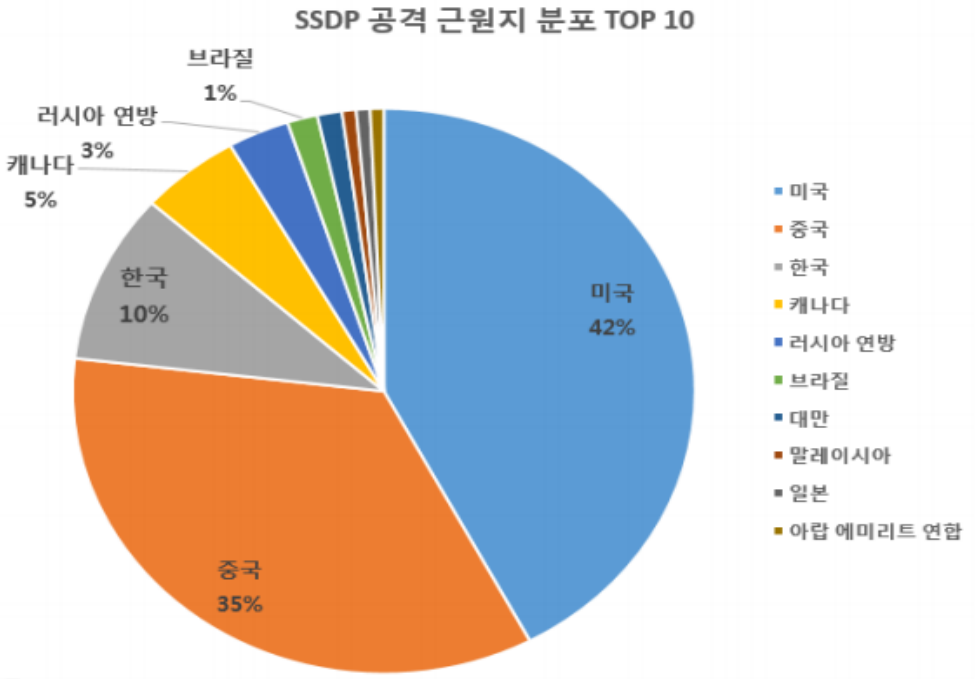
4. Response information size of devices

2. IoT cyber attack trend

▶ Increasing DDoS/DRDoS attack

- Attack stats of SSDP DRDoS

• KISA DDoS 사이버대피소로 발생된 SSDP 공격 IP의 근원지 분포

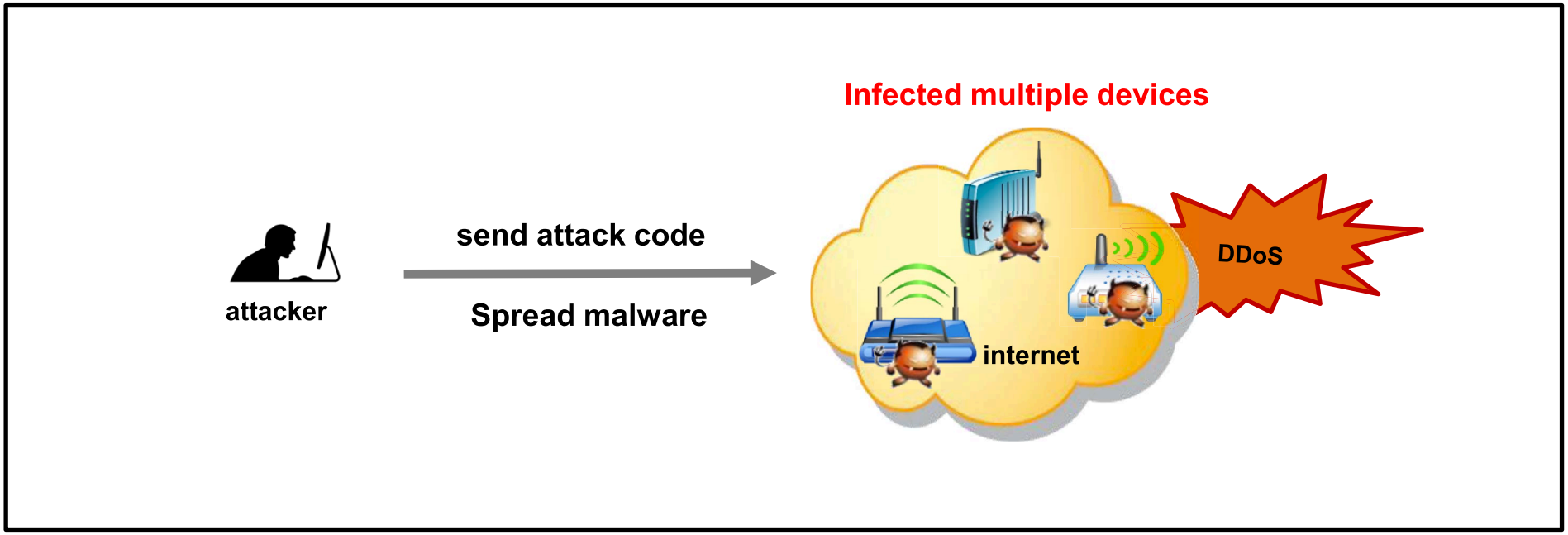


No	국가	개수
1	미국	186,907
2	중국	153,256
3	한국	43,102
4	캐나다	22,992
5	러시아 연방	14,169
6	브라질	6,987
7	대만	5,620
8	말레이시아	3,256
9	일본	3,187
10	아랍 에미리트 연합	3,120
11	우크라이나	3,084
12	홍콩	2,747
13	스웨덴	2,709
14	노르웨이	2,410
15	독일	2,087
16	네덜란드	2,052
17	벨기에	1,970
18	덴마크	1,376
19	스위스	1,080
20	불가리아	944
	------ 중 략 ------	
169	콩고 민주 공화국의	1
170	통가	1
171	팔레스타인 자치 구역	1
172	포클랜드 제도 (말비나스)	1
173	**총합계**	**483,368**

2. IoT cyber attack trend

- Increasing DDoS/DRDoS attack

  - DDoS attack using multiple wireless router



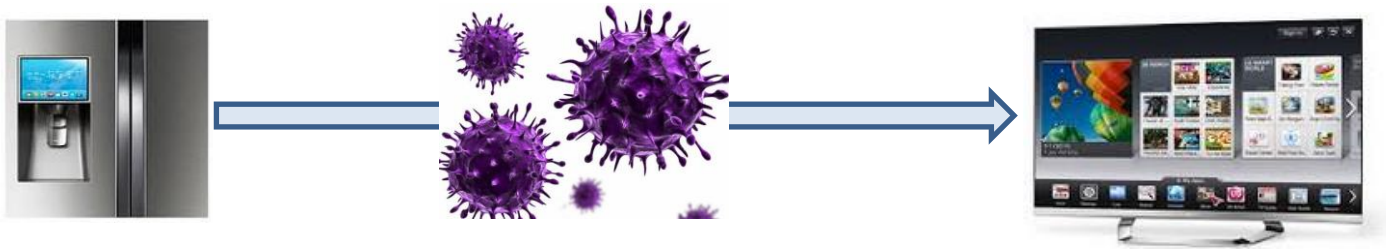
2. IoT cyber attack trend

- Wide Spreading IoT malware

- Improving PC and Server security

- Increase attacker activity against IoT devices

- Worm virus replicates itself through IoT devices



Impact => (zeroday x number of devices)

2. IoT cyber attack trend

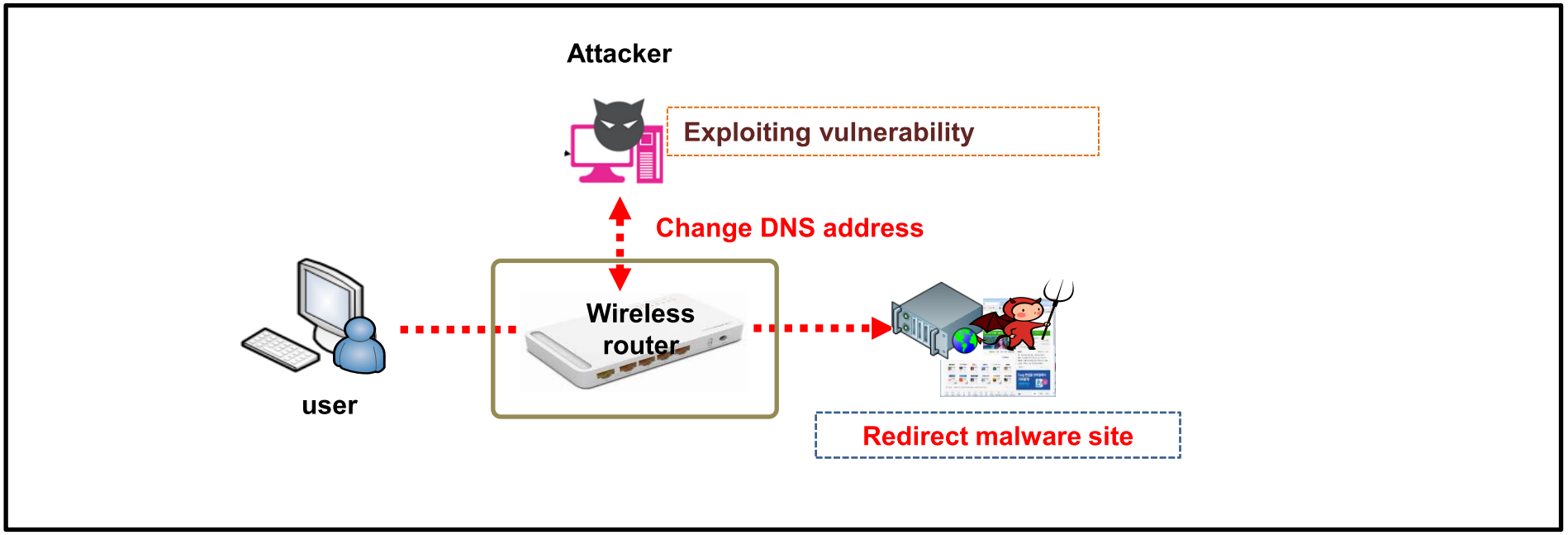
- Large-scale Attack using Automatic Tool

- Exploiting vulnerability, password change, malware infection etc.

2. IoT cyber attack trend

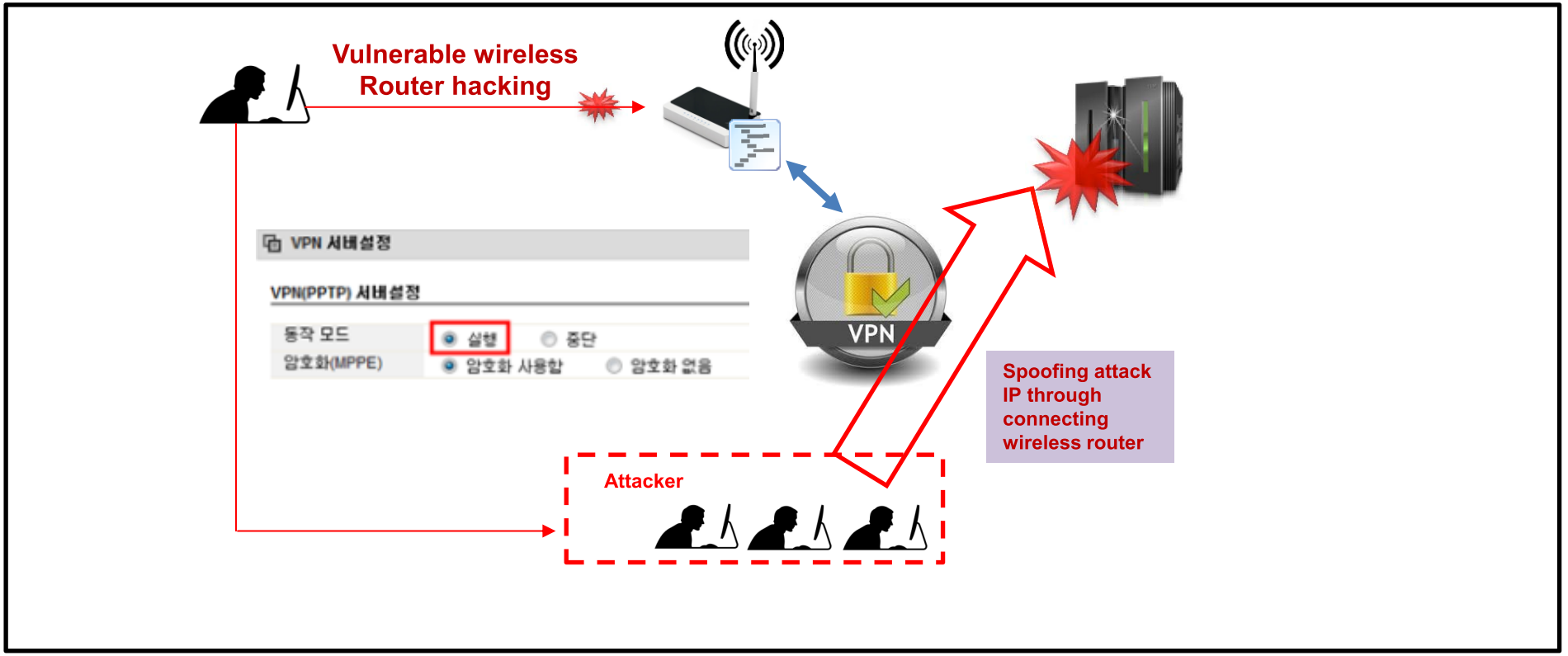
- Phishing and Pharming attack

  - Changing DNS ip address of attacker



2. IoT cyber attack trend

Spoofing attack IP with Compromised wireless router



3. Countermeasure

- Offering minimum service required for external port
- Secure coding in design phase of IoT devices
- Enhancing default security setting option of IoT devices
- Protect private information in communication through IoT devices
- Provide security updates environment of IoT Software
- Enhancing Security for IoT Service infrastructure(Access control etc.)
- Come up with measures for accountability and countermeasure for Security Incident Response of IoT

Thank you.