**과제 제안요청서**

**1. 테마 공모명 : IoT(Internet of Things) Security**

**2. 추진 배경 및 공모 목적**

 **(IoT 시대의 도래)** 사람, 사물, 공간, 데이터 등 모든 것이 인터넷으로 서로 연결되어 정보가 생성·수집·공유·활용되는 IoT 시대에 진입함.

 - '20년에는 260억 개의 사물(Thing)이 인터넷에 연결됨으로서, '13년 대비 연결된

 사물이 10배 이상 증가할 것으로 예측되고 있어(출처: 가트너2013), 모든 사물이

 연결되는 과정에서 공공, 산업 및 개인 생활 전 분야에 창조적 혁신을 유발할 것임.

 - IoT는 '20년까지 전 세계 기업 총 이익을 21% 성장시키는 잠재력을 지닌 기술로

 향후 10년간 19조 달러의 경제효과가 창출될 것으로 추정됨 (Cisco, 2013).

 **(IoT 의미 및 범위)** IoT에서는 응용 및 서비스 분야별로 센서를 중심으로 하는 독자적인

 시스템으로 데이터를 수집하고 활용하던 USN/M2M 등의 파편화된 방식에서 진화하여

 서로 다른 영역/도메인간에서 사용되는 Thing들이 복합적으로 상호운영 되는 방식을

 의미함.

 - Thing은 센서를 중심으로 하는 데이터 수집기능에서 발전하여 액츄에이션 등의

 제어 기능을 포함하며, 처리 기능이 보강된 작은 컴퓨팅 기기로 발전함.

 - 컴퓨터가 인터넷을 통해 자유롭게 연결되듯, 한정된 분야의 응용이나 기업의

 시스템에 연결되는 폐쇄시스템에서 벗어나, Thing 들 간의 통신이나 협업이

 이루어지거나, 필요에 따라 다양한 플랫폼에 연결되는 개방형 시스템으로 발전함.

 **(IoT Security의 중요성)** Thing, 플랫폼 혹은 서비스의 상호 운용이 증대됨에 따라

 IoT 보안은 IoT의 확산 및 성공을 위해 표준화와 함께 필수 불가결한 요소가 됨.

 - IoT는 공공 인프라 및 산업 시설의 정보를 통제할 수 있으므로, 해킹이 일어날 경우

 경제적, 산업적 피해뿐만 아니라 인명적으로도 심각한 피해가 유발될 수 있음.

 - IoT는 개인 정보 유출 등 프라이버시 침해의 정도가 현재와 비교할 수 없을 정도로

 증폭될 가능성이 있음.

 **(공모 목적)**

 - 당 미래기술육성사업은 국내 과학기술의 발전을 통해 인류사회에 공헌하기 위한

 목적으로 '13년 하반기부터 자유 공모를 시행하고 있으며, 이에 대한 보완책으로

 본 테마 공모를 시행함.

 - 테마 공모 주제는 자유 공모에서 커버하지 못하거나 시의 적절한 분야를

 대상으로 연구 커뮤니티의 협조를 통해 선정함.

 - 금번 테마 공모의 주제인 IoT Security 는, 도래하는 IoT 사회에서

 필연적으로 발생할 수 있는 사생활 침해 등 보안 문제에 대해 사전에 점검하고

 해결 방안을 도출함으로써 IoT 산업의 국가 경쟁력을 강화하는데 기여하고자 함

**3. 공모 분야**

  **3.1 시나리오 예시: 분야별 IoT 환경에서 발생할 수 있는 보안 위협에 대한 예시임.**

 (예시1) 주요 기반시설에 대한 공격은 단순한 가상적 시나리오가 아니며 막대한

 피해를 야기한 사례가 이미 존재함. 대표적인 예로 Stuxnet 웜바이러스가 있음.

 Stuxnet은 이란 핵발전시설의 원심분리기 고장을 목표로 설계됨. 2010년 해당

 제어 SW에 침투하여 원심분리기 회전수를 주기적으로 1,410 Hz, 2 Hz, 1,064 Hz로

 변경하여 과부하로 인한 기계고장을 발생시킴. 이는 기존 바이러스와는 달리 물리

 시스템의 특성을 활용한 사이버-물리 융합공격으로 사이버 보안만으로는 감지가

 매우 어려움.

 (예시 2) 차량에 지능형 센서, 통신 등ICT기술 도입이 확대됨에 따라 차량 및

 교통시스템이 소위 스마트 차량 및 교통시스템으로 진화하고 있으며, 이에 따라

 안전성 보장 및 서비스 질 향상을 지향하는 각종 미래지향적 애플리케이션들이

 등장하고 있음. 이러한 차량의 지능화 및 통신기능 탑재는 안전성 및 편의성을

 획기적으로 증대시킬 수 있는 반면, 차량의 대부분의 기능을 악의적으로 원격

 조종할 수 있음을 의미하므로(차량 내부 네트워크 해킹, 브레이크∙스티어링휠

 조종, GPS 위조 등) 차량 및 교통시스템 보안 측면에서 새로운 위협요인을 제공함.

 (예시 3) IoT의 단말을 구성하는 요소 중에는 기존에 이미 인터넷에 연결된 스마트

 기기와 새로이 인터넷에 연결되는 기기가 있을 것임. 기존의 스마트 기기는 이미

 많은 보안 위협을 경험하였으므로 그에 대한 대비책이 어느 정도 마련되어 있다면,

 새로 인터넷에 연결되는 기기는 잠재적인 위협은 존재하지만 어떤 형태의 위협이

 존재하는 지에 대해 많이 알려지지 않았으므로 그에 대한 대응책 마련은 미흡함.

예를 들어 최근에는 스마트 홈 기술의 일환으로CCTV 역할을 함께 하는 로봇

청소기들이 시장에 나와 있지만, 이런 CCTV 를 통해 집 구석구석을 볼 수 있는 기기가

해킹을 당하면, 사생활 침해 및 나아가서는 범죄의 용도로 악용될 수 있을 것임.

(예시 4) 스마트 팩토리는 IoT의 Thing 들의 협업에 의해 운영이 됨. 이 thing 들은

 공장내부의 각종 기기들과 환경 및 건물 시설을 포함하여 신뢰할 수 있는 관리 체제를

 형성하여 실시간 협업에 의해 각 기기의 상태 및 환경에 맞추어 생산을 함.

 스마트 팩토리는 공장 내부의 Thing뿐만 아니라 전력 수급 상황, 기상 상황 및 자재

 조달 상황 등을 인지하는 외부의 Thing등과의 협업을 수행하며, 직원들이 소유한 각종

 Thing, 고객의 요구 등 다양한 플랫폼등과도 협업에 의해 자율적으로 운용됨. 공장

 시설은 신뢰관계에 있는 thing들 내에 악성Thing의 침투로 인해 해킹공격에 쉽게 노출

 될 수 있음. 해킹은 공장시설의 악성 Thing으로 인한 신뢰 관리 손상으로 인한 실시간

 처리 지연만으로도 오동작은 물론 시설의 파손과 인명손실도 유발할 수 있음.

 (예시 5) 병원 내부 망에 침투한 후에 진통제, 항암제, 항생제 등의 자동 투약장치

 (drug infusion pumps)를 원격에서 조작하여 투약 양을 조절하거나, 블루투스 기반의

 제세동기(defibrillators)를 조작하여 긴급한 때 작동을 못하게 할 수 있는 위협이

 확인되었음. 진단 장치를 해킹하여 허위 자료가 의료기록부에 기록되도록 하고,

 의료기기를 정지시키거나 재 구동되게 하여 시스템을 초기화 하는 것이 가능함.

 IoT 환경이 보편화되면 이러한 의료기기들이 모바일 기기들로 보편화되어 지금까지

 확인된 위협들이 보다 현실화 될 전망임.

 **3.2 공모 대상 카테고리: 아래 예시 중에서 1개 이상의 카테고리가 포함되도록 제안**

 **해야 하며, 제안한 내용이 Total Solution 관점에서 어떤 역할과 기여를 하는지**

 **제시해야 함.**

 - Privacy Protection 암호화 방식: 특히 단순화된 소형 device에서 활용 가능한

 light-weight encryption 및 실시간 encryption 고려

 - Device to Device authentication: 종래의 서버를 활용한 KEY 혹은 인증서 확인

 방식은 모든 사물이 연결되는 IoT 환경에는 맞지 않으므로 IoT 환경을 고려한

 사람이 배제된 인증방식 고려

 - Secure Booting: 부팅 시에 디바이스 integrity 또는 디바이스에서 실행될

 소프트웨어에 대한 authenticity와 integrity를 검증할 수 있는 방안

 - VPN: 소형 디바이스들이 서버와 IoT 간 공중망을 사설망처럼 사용할 수 있는 방안

 - Updates and Patches: 다수의 디바이스들이 동작하는 중에 대역폭의 낭비, 성능

 저하, 기능적 안정성에 손상을 가하지 않으면서 보안 패치 또는 업데이트 할 수

 있는 방안

 - Firewalling and IPS: 특정 산업 분야에서 적용될 DPI(Deep Packet Inspection)

 또는 패킷 필터링 방안(Inbound/Outbound)과 악성 침해 행위가 한 단말에 발생시

 그 대응을 전체 IoT 네트워크 시스템 상에서 이뤄지는 집단 지능 기반의 악성 행위

 탐지 및 방어하는 방안

 - Big data Privacy Protection: IoT 또는 IoT 로부터 수집된 데이터에 대한

 프라이버시 보호 또는 익명화 방안

 - 신뢰도 관리: 도메인내 혹은 다른 도메인간의 IoT 망에서 IoT 신뢰도에 따라

 정보를 신뢰하거나 거부하는 등 신뢰도를 관리하는 방안 고려

 - IoT 망 악성 트래픽 탐지 및 대응: IoT 망의 서비스 거부 공격을 막기 위해 악성

 트래픽을 탐지하고 대응하는 기술

 - Fully distributed Security: IoT 들 간에 분산된 security 암호화 및 관리 기술

- 사이버- 물리 융합공격 대응: 디바이스와 시스템의 물리적 특성을 고려한 다양한

공격에 대한 방어, 탐지, 복원시키는 방안

- Access Control & IoT : 특정 공간에 들어온 사용자(Device)의 접근레벨에 따라서

제공하는 정보 및 Control이 가능한Device의 범위를 제한해서 제공하는 환경 구축

- Usable Security and Privacy : 사용자에게 Security 와 Privacy를 인지시키고

 보안 강화를 유도

 ※ 위에 제시된 카테고리 外 새로운 카테고리 제안도 가능하며, 이때는 새로운

 카테고리 제안의 사유와 중요성을 명확하게 제시해야 함.

**4. 요구조건 (연구 제안서에 포함되어야 할 내용)**

 **4.1 연구 목표 및 내용 작성 시 고려사항**

 - 연구제안자가 선택한 분야의 현황 및 문제점, 해결방안을 시나리오 예시 등을

 통해 작성한 후 제안과제가 달성해야 할 수준을 스스로 목표를 확립하고 이에

 대한 평가기준을 작성해야 함

 - 사물인터넷에 연결되는 단말들은 특정 임무수행에 맞게 연산 능력이 최소화

 되도록 설계되며, 에너지, 저장 공간 등의 보다 큰 성능 제약 조건을 가지게

 되므로 제안 내용은 사물인터넷의 다양한 단말 시스템의 특성을 고려한 성능에

 최적화된 보안 솔루션을 제공해야 함

- 제안 내용은 IoT가 일반화되면 서비스 요구에 따라 디바이스 연결부터 구동되는

 서비스까지 일련의 작업이 주변 환경의 현재 상황과 서비스 특성에 따라 다양한 보안과

 Trust level 이 정해지는 부분이 challenge 중의 하나이기에 '사용자의 현재 상황에

 따라 적응적(또는 가변적)으로' 사물인터넷 시스템의 단말들이 가져야 적정한 보안

 수준과 성능 요구 조건을 만족하는 보안 솔루션을 제시하여야 함.

 - 기술적 수준과 목표가 적정하고 개발 목표가 해당 산업의 기술력 향상을 유도할

 만큼의 도전성이 있어야 함

 - 국내외 기술과 비교할 때 연구개발 내용이 차별성과 혁신성이 있어야 함

 **4.2 평가방안 제시 : 제안자는 연구결과물의 검증 방법과 평가방법을 제시해야 하며,**

 **선택한 사유와 함께 정량적인 평가지표를 제시**

- 연구결과의 검증방법이 구현인지 또는 시뮬레이션인지 선정

- 기능시험 또는 성능시험 등의 시험 방식을 선정하고 평가지표 제시

**4.3 IoT 환경 하에서의 작동이 가능해야 함**

- 기존 PC와 같은 성능환경이 아닌 제한된 resource(열악한 상황, 즉 에너지가 충분하지

 않고 CPU 성능이 낮거나, 소형화 등의 상황)에서 기능이 제대로 작동됨을 검증해야 함

**5. 신청자격**

 - 국내 대학 교원(전임, 비전임) 및 부설연구소 연구원

 - 공공 연구기관(국공립 및 정부출연연구기관 등) 연구원

 - 기업 부설연구소 연구원(대기업 계열 제외)

**6. 지원규모**

 - 기간 및 연구비 : 과제별 3년 이내 / 과제별 총 10억원 이내

 ※ 과제별 연구기간과 예산, 연구진 구성은 연구자가 합리적으로 제안

**7. 과제신청 및 심사**

 - 접수 기간 : '14년 6월 14일(토) 08:00 ~ 6월 27일(금) 17:00까지

 - 신청 방법 : 센터 홈페이지에「연구제안서」등록

 ※ 연구책임자 본인의 명의로 회원 가입을 하고 과제를 접수하여야 합니다.

 - 심사 절차

 ·국내 석학 및 전문가로 심사위원단 구성

 ·서면 심사 선정과제에 한하여 발표 심사 진행, 필요 시 현장 실사 실시

 - 주요 심사포인트: 연구 독창성과 탁월성을 절대평가 방식으로 심사

 ·서면심사 : ① 연구의 독창성 또는 혁신성, ② 기술·산업·사회적 Impact,

                   ③ Feasibility

     ·발표심사 : 서면심사 심사항목에 추가하여 연구계획의 적절성, 연구진 역량

**8. 진행 일정**

 -『연구제안서』접수 '14년 6월 14일(토) 08:00 ~ 6월 27일(금) 17:00

- 서면 심사 결과 발표 '14년 7월 14일(월)

 -『발표자료』접수 '14년 7월 22일(화) 12:00

 - 발표 심사 '14년 7월 25일(금)

 - 선정 과제 발표 '14년 8월 28일(목)

 - 과제 협약 및 연구비 지급 '14년 9월 中

**9. 과제 관리**

 - 연구자가 제안한 Milestone을 기본으로 과제 진척현황 공유와 평가 실시

**10. 기타**

 - 자격요건, 연구비 등 관련 내용은 홈페이지의 FAQ를 참조바랍니다.

 연구제안서 양식은 홈페이지 테마공모에서 다운받으시면 됩니다.

 (삼성전자 미래기술육성센터 홈페이지: http://www.samsungftf.com)

 - 관련 문의는 삼성전자 미래기술육성센터 윤재원 과장에게 연락바랍니다.

 (이메일 : creative.ftf@samsung.com, 전화 02-2255-0642)

 - 이상 -