

IoT 보안에 대한 국내외 연구 동향 분석

유 우 영*

요 약

IoT 기술은 현재 다양한 산업 현장에서 적용되고 있으며, 제4차 산업혁명에서 핵심 기술로 발전되고 있다. IoT의 발전과 함께 IoT 보안에 대한 인식과 중요성이 증가하고 있으며, 이러한 보안 위협에 대응하기 위해 IoT 보안에 대한 연구가 진행되고 있다. 그러나, 거시적인 측면에서 IoT 보안 인식을 위한 연구 동향 분석은 미흡한 상황이다. 본 논문은 현재까지 진행된 국내외 IoT 및 IoT 보안에 대한 연구 동향을 분석하여 개선사항을 도출하는 탐색적 연구이다. 연구 범위는 보안 분야를 주요 주제로 다루는 국내외 저널의 229개 논문을 대상으로 분석하였다. 이 중에서 IoT 보안과 관련성이 높은 96개 논문에 대해서는 상세 분석을 수행하였다. 연구 결과 IoT 보안에 대한 동향 분석, 인증 및 키 관리, 프라이버시에 대한 연구가 많이 진행되고 있었다. IoT 기술을 적용하는 서비스 특성을 고려한 연구와 IoT 기기간 접근제어 및 인증 등에 대한 세부적인 연구가 필요하며, 국내의 경우 IoT 환경에서의 Privacy 이슈를 다루는 연구가 미흡한 것으로 나타났다.

An Analysis of Research Trends in IoT Security

Yu Woo Young*

ABSTRACT

IoT technology is currently being applied at various industrial sites and is developing as a core technology in the fourth industrial revolution. Along with IoT developments, awareness and importance of IoT security is increasing, and research on IoT security is underway to counter these threats. However, research trends in the context of IoT security awareness are insufficient. This paper is a research that analyzes the progress of R&D and IoT security in both domestic and international IoT and thus leads to improvements. The research covered the 229 papers and articles of domestic and foreign journals covering security fields as a main theme. Among them, detailed analyses of 96 papers related to IoT security were performed. Research has shown that many studies are being conducted on trends in IoT security, key management and privacy. A detailed study on the characteristics of services to apply IoT technologies and access control and authentication between IoT devices is needed, and a study that addressed the issues of privacy in IoT environments in Korea

Key words : IoT Security, Internet of things Security, IoT, Internet of Things

접수일(2018년 1월 30일), 게재확정일(2018년 3월 23일)

* 중앙대학교/융합보안학과

1. 서 론

인터넷과 정보기술의 발전이 우리의 생활환경을 급격히 변화시키고 있다. 특히 사물인터넷(Internet of Things, 이하 IoT)은 제4차 산업혁명의 중심에서 중요한 역할을 수행할 것으로 예측되고 있으며, 헬스 케어, 자동차, 가전, 공장 및 전력망 등 다양한 분야에서 산업의 성장을 위한 핵심 기술로 간주되고 있다. 노키아(2015) 분석에 따르면 2025년까지 IoT 접속기기의 수는 약300억 개까지 증가할 것으로 예상된다[3]. IoT의 개념은 1999년 케빈 애쉬톤(Kevin Ashton)이 최초로 정의하였으며, 2016년 다보스 포럼에서 클라우스 슈바(Klaus Schwab) 회장은 제4차 산업 혁명의 중심에 빅-데이터, AI(인공지능), IoT 등이 핵심 기술이 될 것이라고 했다.

IoT의 폭발적인 발전과 달리 실제 사용자들의 인식과 이용도가 낮은 편인데, 이는 IoT 기기에 대한 오류, Privacy 이슈, 해킹 등의 보안에 대한 문제가 가장 큰 것으로 나타났고, 새로운 기술에 대한 거부감도 존재하는 것으로 나타났다[1][2]. IoT가 산업의 중심에서 핵심 기술로 발전하면서 보안에 대한 우려가 있고 이에 대한 연구의 필요성은 대두되고 있어, IoT 보안 연구에 대한 방향성을 분석할 필요가 있다.

본 논문에서는 현재까지 진행된 IoT 보안에 대한 국내의 연구 동향을 분석하여 시사점을 도출하고, IoT 보안에 대한 연구 방향을 제시하고자 한다. 제2장에서는 IoT 동향 분석 방법을 설명하고, 제3장에서는 국내외 IoT 보안 연구 동향을 분석한다. 제4장에서는 연구 결과에 대한 시사점을 도출하며, 제5장에서는 결론을 정리하고 향후 IoT 연구의 발전을 위한 방향성을 제언한다.

2. 연구 방법

IoT 보안에 대한 연구 동향 분석을 위해 M.T. Dlamini[4], Kunwoo Kim[5], Mario Silic과 Andrea Back[8]의 연구 방법을 참고하여 IoT 보안

연구와 관련이 높은 해외 IoT 관련 논문으로는 Computer Networks, Computer(IEEE), Computer & Security, International Journal of Security and its Applications, Security and Communication Networks 등 5개 저널을 선정하였고, 국내 IoT 연구 동향 분석을 위해 국내 정보보호 분야의 대표적인 연구기관인 한국정보보호학회의 논문지와 학회지, 한국융합보안학회, 한국인터넷정보학회, 한국정보처리학회, 한국IT서비스학회 등 국내 5개 연구기관의 논문지와 학회지를 대상으로 선정하였다.

IoT 보안에 대한 연구 논문은 분석 대상은 제목과 키워드에 IoT, IoT Security를 검색 조건으로 논문을 수집하였다. 제목과 키워드로 논문을 검색한 이유는 제목에는 IoT 또는 Security가 포함되어 있지 않으나, 논문의 내용에 IoT, Security가 포함되는 경우가 존재하기 때문이다.

IoT 보안 연구 동향 분석을 위한 분류 기준은 한국인터넷진흥원(2013)에서 제시한 IoT 3대 주요기술인 센싱기술, 네트워크 인프라 기술, IoT 서비스 기술과 IRS Global(2014)에서 IoT 시장 동향 분석에 사용된 분류 기준인 디바이스, 네트워크, 시스템 사업, 어플리케이션 및 서비스 분류 등을 살펴보면 다양한 기술적 계층으로 IoT가 구성되어 있음에도 불구하고, 다음과 같이 3가지 기술영역으로 구분할 수 있다.

<표 1> IoT Technology Classification

Category	Contents
Device	Sensors, Processors, OS etc
Connectivity	WiFi, 3G/4G, Bluetooth, Ethernet etc
Platform	Big-Data, Cloud, Security, Privacy, Application, Smart Grid, Smart home, Health-care etc

첫째, IoT 기기에 내제되어 있는 센서, 마이크로프로세서, 연결 모듈, 운영체제 등을 포함되는 제품(Device) 부문. 둘째, 이러한 제품(Device)을 유무선 네트워크로 연결하고 인터넷에 접속할 수 있게 하는 통신(Connectivity)부문. 셋째, 통신 연

결을 통해 정보의 생산을 위해 데이터를 수집 · 축적 · 분석 · 활용 할 수 있도록 정보 생성 및 분석의 기반 기술들을 제공하는 플랫폼(Platform) 부문으로 구분할 수 있다.

3. 국내외 IoT 보안 연구 동향 분석

3.1 기본 분석

국내의 IoT 논문을 분석한 결과 Device 관련 연구는 17건(7.4%), Connectivity 관련 연구는 25건(10.9%), Platform 관련 연구는 187건(81.7%)으로 Platform 관련 연구가 가장 많았으며, 저널별 논문 발표 건수는 <표 2>와 같다.

<표 2> Publications Status

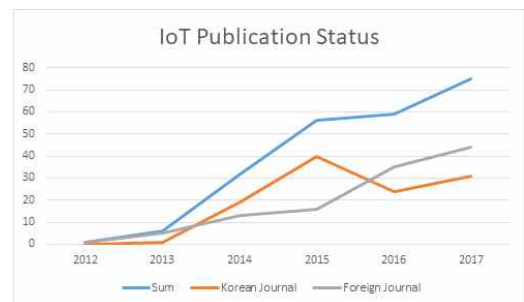
Category		Device	Connectivity	Platform	Sum
Korea	Convergence security journal	-	1	7	8
	Journal of Internet Computing and Services	1	2	12	15
	Journal of the Korea Institute of Information Security and Cryptology	1	3	15	19
	KIPS transactions on computer and communication systems	4	4	36	44
	Korea information processing society review	-	-	9	9
	Korea Society of IT Services	1	-	10	11
	Review of KIISC	-	1	9	10
Sub Sum		7	11	98	116
Foreign	Computer Networks	2	4	16	22
	Computer(IEEE)	5	4	23	32
	Computers & Security	1	1	10	12
	International Journal of Security and Its Applications	-	3	22	25
	Security and Communication Networks	2	2	18	22
	Sub Sum		10	14	89
Sum		17	25	187	229

분석 대상 논문 229개 모두 제목과 키워드 검색으로 분석 대상을 선별하였지만, 내용상 보안과 관련성 떨어지는 SW 및 HW 개발, 데이터 처리, 네트워크 디자인이나 센서 기술 등의 내용이 포함된 논문이 다수 포함되어 있어 보안과 관련성이 높은 논문을 분류하였다. IoT 관련 연구 229개 논문을 대상으로 전체적인 IoT 연구 동향을 파악한 후, IoT 보안 관련 논문을 대상으로 상세 분석을 수행하였다.

IoT 관련 연구는 2014년부터 급격히 증가하고

있는데, 연도별 발표 건수도 2012년(1건), 2013년(6건), 2014년(32건), 2015년(56건), 2016년(59건), 2017년(75건)의 연구가 진행되었다.

IoT 관련 연구는 매년 증가하고 있는 추세이며, 국내 연구의 경우 2015년을 정점으로 IoT 관련 연구가 감소하였다 다시 증가하고 있으며, 해외의 경우 지속적으로 연구가 증가하고 있는 추세이다.



(그림 1) IoT Publication Status

3.2 상세 분석

3.2.1 IoT 연구 동향

연구 주제를 살펴보면 보안 관련 연구가 전체 IoT 연구의 41.9%(96개)으로 IoT 보안에 대한 연구가 가장 많았으며, 다음으로 SW Development 9.2%(21개), Data Processing 6.6%(15개), Sensors 6.6%(15개) 등으로 연구가 진행되었다.

<표 3>. IoT Research

Research Theme	% of Research (Number)
Security	41.9%(96)
SW Development	9.2%(21)
Data Processing	6.6%(15)
Sensors	6.6%(15)
Analysis of Trend	4.4%(10)
Health care	3.9%(9)
Network Design	3.9%(9)
Smart Grid	3.5%(8)
Protocol Design	3.5%(8)
etc	16.6%(38)

IoT 보안 연구에 대한 개선사항을 도출하기 위해 29개 연구 논문 중에서 보안과 관련성이 높은 96개 논문(국내 37개, 해외 59개)을 대상으로 상세 분석을 수행하였다. 국내 116개 IoT 연구 논문 중에서 보안에 대한 연구는 37개 31.9%, SW Development 12.1%(14개), Data Processing 9.5%(11개), Health care 6.9%(8개) 비율로 연구되고 있다.

<표 4> Korean IoT Research

Research Theme	% of Research (Number)
Security	31.9%(37)
SW Development	12.1%(14)
Data Processing	9.5%(11)
Health care	6.9%(8)
Sensors	6.0%(7)
Smart Grid	5.2%(6)
Protocol Design	5.2%(6)
Context Awareness	4.3%(5)
Service Operation	4.3%(5)
etc	14.7%(17)

해외 IoT 연구 113개 논문 중 보안과 관련된 연구

는 52.2%(59개), Sensors 7.1%(8), Analysis of Trend 6.2%(7개), SW Development 6.2%(7개), Network Design 5.3%(6개) 등의 순으로 연구가 진행되고 있다.

국내에서도 보안이 가장 중요한 연구 주제이지만, 해외의 경우 국내 보다 보안에 대한 연구가 (+)20.3% 더 활발히 진행되고 있음을 알 수 있다.

<표 5> Foreign IoT Research

Research Theme	% of Research (Number)
Security	52.2%(59)
Sensors	7.1%(8)
Analysis of Trend	6.2%(7)
SW Development	6.2%(7)
Network Design	5.3%(6)
HW Development	4.4%(5)
Data Processing	3.5%(4)
etc	15%(17)

3.2.2 IoT 보안 연구 동향

IoT 보안 연구 동향 분석을 위한 분류는 NIST의 Cybersecurity Framework을 참고하고, 연구 논문의 키워드 분석을 통해 선별하였다. 보안에 대한 문제를 제시하였지만 해결책이 명확하지 않고 방향성만 제시된 경우 Analysis of Trend로 분류, 취약점 분석 및 위협 분석 등 유사한 내용은 Security analysis로 분류, 네트워크 전송, 분산 네트워크 구성 등의 연구는 Network Security로 분류, 보안 미유 및 정책 제안, 기술 및 운영 표준화 등은 Policy and Standardization으로 분류하였다.

IoT 보안에 대한 96개 논문을 분석한 결과 Analysis of Trend 17.7%(17개), Authentication and Key exchange protocol 16.7%(16개)로 가장 많은 연구가 진행되었으며, Privacy 15.6%(15개), Policy and Standardization 11.5%(11개), Security analysis 8.3%(8개), Network Security 6.3%(6개), Intrusion Detection 5.2%(5개) 등으로 연구되고 있다. 이머징 기술의 특징을 반영하듯, 문제 발굴 및 방향성 제시하는 연구가 가장 많았으며, IoT의 기술적 특성을 반영한 인증 및 키 교환, IoT 보안에 대한 정책 및 표준화 제안 등의 연구도 많이 진행되고 있다. 특히, Network

k Security 부문에서는 저전력 경량 디바이스 환경에서의 연구가 진행되고 있다.

<표 6> IoT Security Research

Research Theme	% of Research (Number)
Analysis of Trend	17.7%(17)
Authentication and Key exchange protocol	16.7%(16)
Privacy	15.6%(15)
Policy and Standardization	11.5%(11)
Security analysis	8.3%(8)
Network Security	6.3%(6)
Intrusion Detection	5.2%(5)
Encryption Design	4.2%(4)
Access Control	4.2%(4)
Side Channel Analysis	3.1%(3)
DDoS	2.1%(2)
Sensors Security	2.1%(2)
Medical Information Security	2.1%(2)
Payment System	1.0%(1)

국내 IoT 보안 연구는 Analysis of Trend 27.0%(10), Authentication and key exchange protocol 13.5%(5). Policy and Standardization 13.5%(5) 등이 전체 50% 이상의 비중으로 연구가 진행되었으며, 해외 연구는 Privacy 22.0%(13), Authentication and key exchange protocol 18.6%(11), Analysis of Trend 11.9%(7), Policy and Standardization 10.2%(6) 등의 순으로 연구가 진행되었다. 국내와 해외 연구에서 많이 차이 나는 점은 국내에서는 Analysis of Trend 연구가 해외보다 (+) 15.1% 더 진행되었으며, 해외에서는 Privacy에 대한 연구가 (+)16.6% 더 많이 진행되었다.

<표 7> Korean IoT Security Research

Research Theme	% of Research (Number)
Analysis of Trend	27.0%(10)
Authentication and Key exchange protocol	13.5%(5)

Policy and Standardization	13.5%(5)
Side Channel Analysis	8.1%(3)
Security analysis	8.1%(3)
Privacy	5.4%(2)
Sensors Security	5.4%(2)
Medical Information Security	5.4%(2)
Access Control	5.4%(2)
Intrusion Detection	2.7%(1)
Payment System	2.7%(1)
Network Security	2.7%(1)

Network Security와 Access Control 관련 연구는 보안에 초점이 맞추어져 있지 않고, IoT 기술의 특성을 반영하여 게이트웨이를 이용한 효율적인 보안과 접근제어 구현을 위한 연구가 진행되었다.

<표 8> Foreign IoT Security Research

Research Theme	% of Research (Number)
Privacy	22.0%(13)
Authentication and Key exchange protocol	18.6%(11)
Analysis of Trend	11.9%(7)
Policy and Standardization	10.2%(6)
Security analysis	8.5%(5)
Network Security	8.5%(5)
Intrusion Detection	6.8%(4)
Encryption Design	6.8%(4)
DDoS	3.4%(2)
Access Control	3.4%(2)

4. 연구 결과 및 시사점

4.1 연구 결과

국내외 IoT 보안 관련 연구 동향을 분석한 결과 국내의 경우 해외에 비하여 보안에 대한 동향 분석, 보안 이슈 제시, 정책적인 방향성 제시 등의 연구가 많았으며, 실제 IoT 환경을 구축하기 위해 필요한 인증, 접근 제어, Privacy 등에 대한 연구는 부족한 부분이 있었다. 연도별 연구 동향 분석 결과에서는 국내 연구는 2015년을 정점으로 연구 건수가 감소하는 추세이지만, 해외의 경우 지속적

으로 IoT 및 IoT Security에 대한 연구가 증가하고 있었다.

연구의 양적인 측면뿐만 아니라 내용적인 측면에서 살펴보면, Network Security의 경우 IoT 네트워크에서 에너지 및 보안의 효율적인 구현과 무선 네트워크에서의 네트워크 보안 구축에 대한 것으로 분산 디바이스 및 다양한 기기가 접속하는 IoT 환경의 특성을 반영하는데 미흡한 부분이 있었으며, 접근제어에 대한 연구 또한 게이트웨이를 이용한 효율성 강화에 초점이 맞추어져 있어 IoT 센서 및 디바이스 제어를 위한 접근 제어에 대한 연구는 미흡한 것으로 나타났다.

국내에서 가장 많이 연구가 진행된 Analysis of Trend 부분을 살펴보면 IoT 산업이 ICT 융합 서비스로써 종합적인 보안 위협에 대한 동향 분석과 IoT 구현사례를 접목한 위협 동향 파악은 세분화되어 연구가 진행되고 있다. 해외의 경우 Privacy에 대한 연구가 가장 많이 진행되고 있는데, 센서 기술을 통해 사용자의 주변 상황 정보를 수집하는 IoT 특성에 따른 Privacy 이슈 문제를 국내보다 더 심각하게 생각하고 연구하는 경향을 보여주고 있다.

국내에서 연구되고 있는 Side Channel Analysis(부채널 공격)에 대한 연구는 IoT 기기가 일반적으로 경량 디바이스의 특성을 가지고 있어 하드웨어적으로 충분한 보안 기능을 구현하지 못하는 경우가 대부분인데, 이러한 취약점을 이용하여 기기의 전자파 신호나 전력 소모량 등을 분석하여 보안을 우회하는 새로운 취약점 분석 방법이다. 현재 생산되는 많은 IoT 기기가 Side Channel Analysis 공격에 취약한 상황으로 IoT 기기 제조사는 생산단계에서 Side Channel Analysis Attack에 대비하는 것이 필요하다. 또한, 접근제어에 대한 연구는 게이트웨이를 이용한 접근의 효율성에 대한 연구인데, IoT 환경에서의 접근 제어는 음성, 데이터 서비스 등을 지원하고 분산된 매체에 대한 접근을 제어하는 기법에 대한 연구가 필요한데[7] 현재까지 진행된 접근제어 논문에서는 이러한 부분에 대한 연구가 미흡한 것으로 나타났다.

4.2 시사점

정보기술의 비약적인 발전과 함께 보안에 대한 위협도 점점 더 지능화되고 고도화되어 보안사고가 지속적으로 발생하고 있으며, IoT와 같이 급성장하는 시장에서는 보안 위협이 더욱 더 크게 증가하고 있다. 이러한 상황에서 IoT에 대한 정보보호 수준을 높이고, 사용자에게 신뢰성 높은 서비스를 제공하기 위해 보안 역량 향상이 매우 중요하며, 보안 역량 향상을 위해 현재 진행되고 있는 보안에 대한 연구 동향을 정확하게 파악하는 것이 매우 중요하여 국내외 연구 논문을 중심으로 IoT Security에 대한 연구 동향을 파악하였다.

연구 결과를 종합적으로 살펴보면 국내에서는 2015년을 기점으로 IoT 보안에 대한 연구가 해외 연구보다 감소하는 것으로 나타나고 있으며, IoT 환경에서의 사용자 및 디바이스 인증, 접근제어, 상호 접속 등 IoT 기술 구현에 필요한 실질적인 보안 기술 보다는 IoT에 대한 동향 파악, 이슈 분석, 정책적인 방향 제시 등의 연구가 많은 것으로 나타나고 있다. 특히, IoT 환경에서는 접근제어 정책의 충돌을 고려한 IoT 플랫폼 구축이 필요한 것으로 연구되었으나[9], 이에 대한 후속 연구는 발견되지 않았다.

IoT 연구의 내용적인 측면에서도 국내 연구는 보안에 대한 정책적이고 동향파악 측면의 포괄적인 내용을 많이 다루고 있었으며, 해외 논문의 경우 기술의 구체적인 구현이나, 프라이버시 이슈 등을 주요한 연구 주제로 다루고 있었다. 국내 IoT 보안 연구의 향후 과제로써 IoT 플랫폼과 서비스 구축을 위해 필요한 접근통제, 디바이스 간 상호인증, 프라이버시 등 기술적인 측면에서의 구체적인 연구가 필요해 보인다..

5. 결 론

본 논문은 보안과 관련성이 높은 국내외 저널의 논문을 대상으로 IoT 및 IoT Security 연구에 대한 동향 분석을 한 것으로 전체 IoT 분야의 연구를 대표한다고 보기에는 어려움이 있으나, IoT Security에 대한 전체적인 연구 동향을 파악하고 시사점을 도출하였다는 점에서 의의가 있다. 본 논문의 연구 결과를

토대로 새롭게 발전하는 IoT 분야에서 보안과 관련된 부족한 후속 연구가 이루어져 국내 IoT 보안에 대한 수준이 향상되기를 기대한다.

본 연구를 수행하며 발견된 시사점을 바탕으로 IoT 보안에 대한 연구 방향을 다음과 제시하고자 한다. 첫째, IoT 서비스는 스마트 그리드, 스마트 홈, 스마트 자동차 등 다양한 산업 분야에 적용되고 있는데, IoT 보안에 대한 연구도 산업별 특성을 고려하여 연구가 진행되어야 할 것이다. 기존 연구에서는 서비스산업별 특성을 고려한 연구가 부족하였으며, IoT 환경은 다양한 기기가 상호 접속하는 환경인데, 이러한 특성이 고려된 접근 제어 정책 적용, 인증 및 암호화 등에 대한 세부적인 연구가 필요해 보인다.

둘째, IoT 환경은 개인의 사생활 침해 우려가 높기 때문에 개인정보보호 및 프라이버시에 대한 연구가 보다 더 적극적으로 수행될 필요가 있는 것으로 판단한다.

셋째, 본 연구는 연구의 접근방법과 특성상 IoT 특허 관련 기술과 소프트웨어 응용 기술 분야에 대한 연구가 미흡한 점이 있는데, 향후 특허 관련 기술과 응용 기술 분야에 대한 연구를 후속 연구로 수행할 계획이다.

참고문헌

- [1] YoonSun, Jin., Ohbyung, Kwon. "An empirical study of the factors affecting IoT use," *Journal of Korea society of IT Services*, pp. 432-435, 2017.
- [2] C. L. Hsu., & J. C. C. Lin., "An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives," *Computers in Human Behavior*, 62, pp. 516-527, Sep. 2016.
- [3] NOKIA, "LTE-M-Optimizing LTE for the Internet of Thing," <http://networks.nokia.com>, White Paper, pp. 1-16, 2016.
- [4] M.T. Dlamini, J.H.P. Eloff, and M.M.Eloff, "Information security: the moving target," *Computers & Security*, vol. 28, no. 3-4, pp. 189-198, Jun 2009.
- [5] Kunwoo Kim, "An Analysis of Research Trends in Information Security Education," *Journal of The Korea Institute of Information Security & Cryptology*, 26(2), pp. 489-499, Apr 2016.
- [6] Gartner Report, "Market Trends: TSP, Must Invest in the Rapidly Evolving IoT Ecosystem Now", Gartner, Mar 2014.
- [7] Mark Taylor, Denis Reilly, et al. "An access control management protocol for Internet of Things devices," *Network Security Volume 2017, Issue 7*, pp.11-17, July 2017.
- [8] Mario Silic and Andrea Back. "Information security: Critical review and future directions for research." *Information Management & Computer Security*, vol. 22, no. 3, pp. 279-308, Jul. 2014.
- [9] Mark Taylor, Denis Reilly, "An access control management protocol for Internet of Things devices." In *Network Security*, 2017(7), pp.11-17, July. 2017.

[저자소개]



유 우 영 (Wool-Young Yu)

2012년 8월 고려대학교
정보경영공학과 석사

2017년 8월 중앙대학교
융합보안학과 박사 수료

email : wooyoung.yu@gmail.com