





웹사이트 보안 및 IoT 보안의 흐름과 대책

DigiCert Ireland Limited, Korea Branch

나 정주 지사장

(Country Manager for Korea, Indonesia, Pakistan and Vietnam)

James.Nah@digicert.com

안 건

SSL 인증서란 무엇인가?

CA/B 포럼

브라우저 시장 동향

SSL 인증서 시장 동향

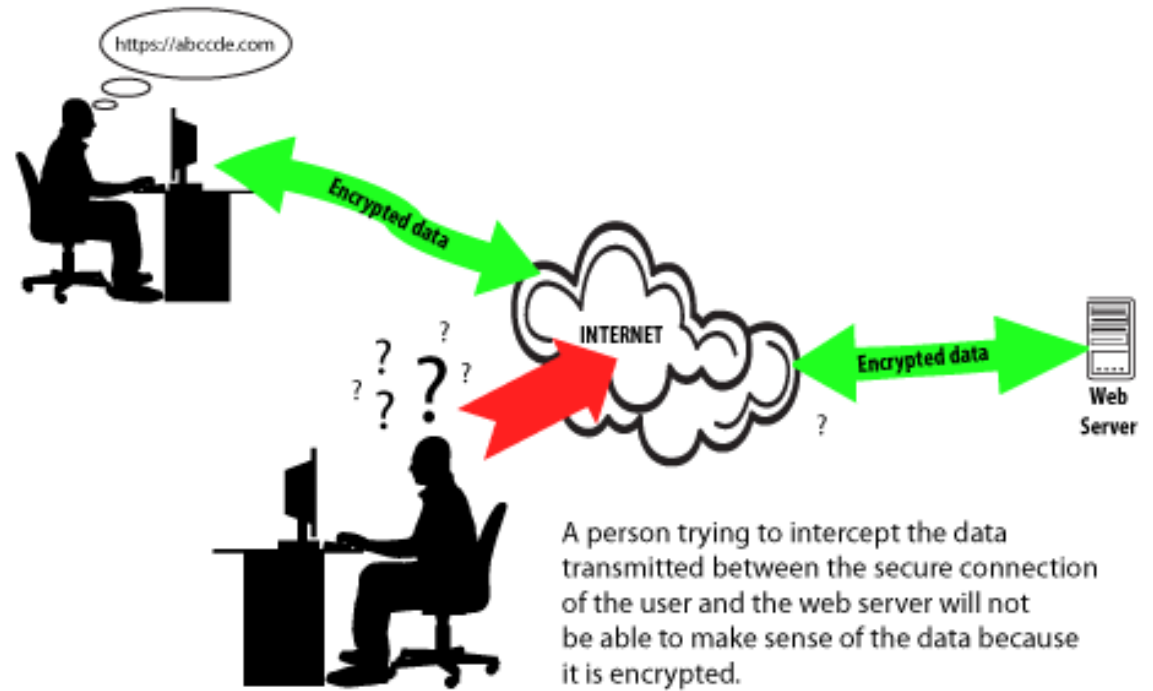
Phishing 업데이트

IoT 동향

회사 소개 – DigiCert & (주)파인앤서비스

SSL 인증서란 무엇인가?

SSL(Secure Socket Layer) 인증서란?



사용자와 웹 서버 간의 데이터는 암호화되어 있기 때문에
중간자가 공격하여 Data를 보더라도 내용을 알 수 없음

SSL 인증서 종류



Domain Validation
Basic Validation



Organizational Validation
Standard Validation

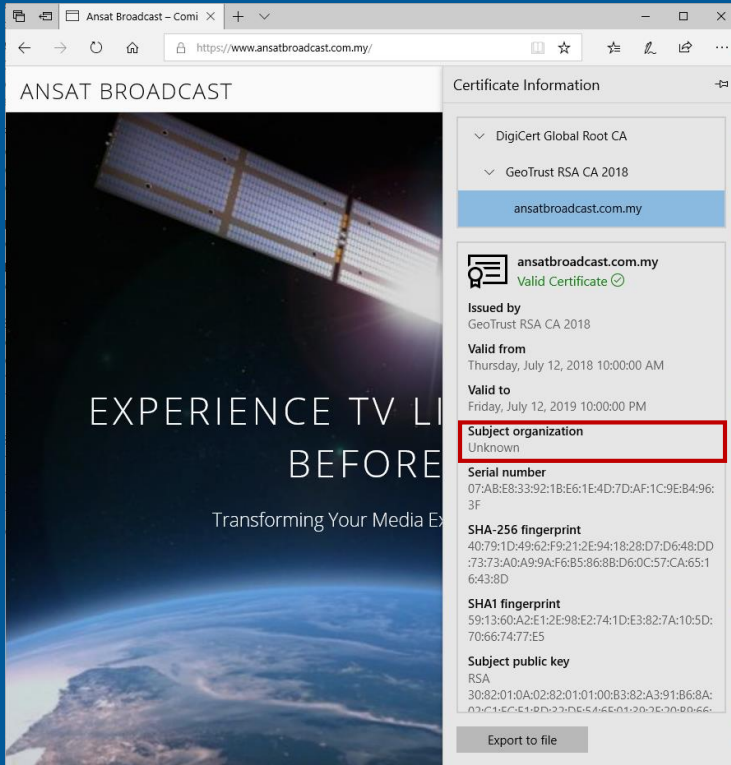


Extended Validation
Enterprise Validation

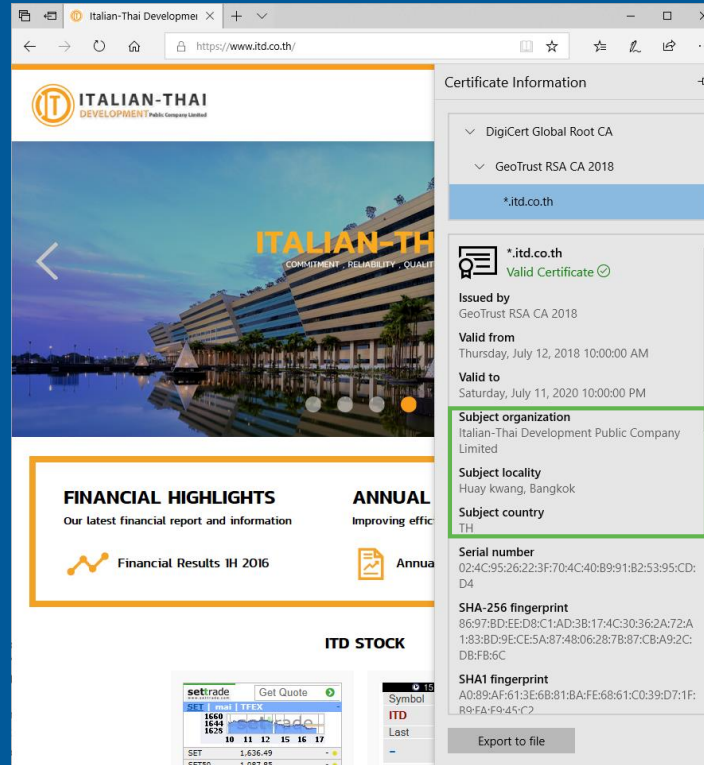


SSL 인증서의 차이

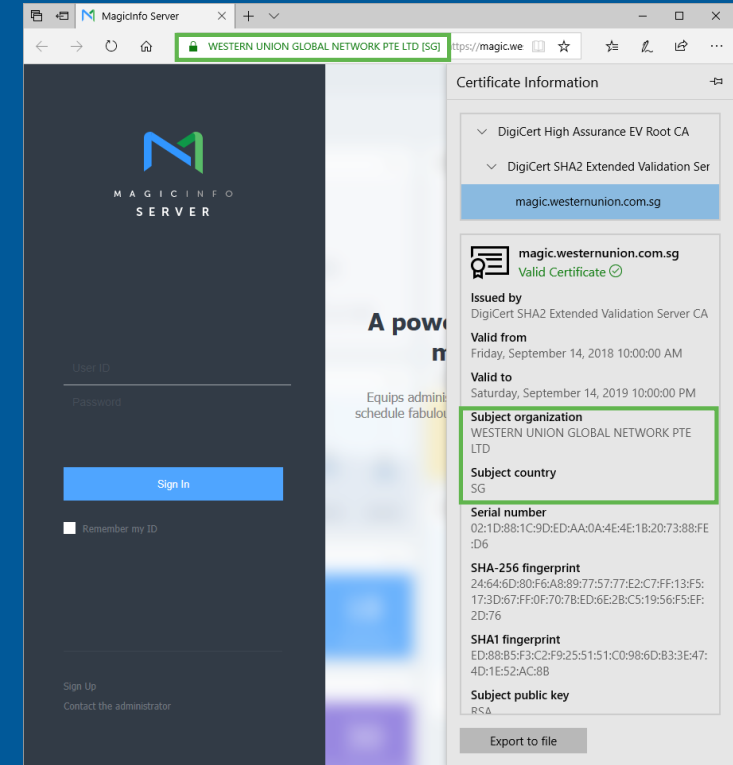
Domain Validation Basic Validation




Organizational Validation Standard Validation



Extended Validation Enterprise Validation



Two overlapping light blue geometric shapes, a parallelogram and a rectangle, are positioned to the left of the text.

HTTPS가 안전하다고 하는 것은 거짓말은 아니지만,
엄격하게 얘기하면, 맞는 얘기는 아니다. HTTPS는 사이버
보안 퍼즐 안에서 그저 간단한 여러 보안 기능들 중 하나일
뿐이다




“Saying that HTTPS is secure isn't false, but it is also not strictly true. It is one piece in a cybersecurity jigsaw that is on the face of it one of the easiest security features to identify”

사례: Cathay Pacific

Secure | <https://www.news.com.au/travel/world-travel/asia/cathay-pacific-spells-its-own-name-wrong-on-side-of-plane/news-story/481f200596162a9d9bd4ae5bcb4a5a9d>

news.com.au


National | World | Lifestyle | Travel | Entertainment | Technology | Finance | Sport



Cathay Pacific spelled its name wrong on the side of a new jet recently. Picture: Twitter/Cathay Pacific Source: Supplied


Ads by Kiosked

THE APPLE HUNT IS ON!




Travellers at Hong Kong International Airport spotted the sign-writer's mistake and contacted the airline immediately.

MORE IN WORLD TRAVEL




UP TO 30% OFF
SITEWIDE#



Conditions apply

Shop Now

Price Match
Guarantee



advertisement

사례: Cathay Pacific

Secure | <https://www.abc.net.au/news/2018-10-25/cathay-pacific-data-breach-affects-9.4-million-customers/10429878>

Sites

ABC

Log In

Search

NEWS

SET LOCATION
for local news & weather

Just In

Politics

World

Business

Sport

Science

Health

Arts

Analysis

Fact Check

More

Print

Email

Facebook

Twitter

More

Cathay Pacific stocks plunge after airline reveals mass data breach by hacker

Updated yesterday at 7:54pm

Cathay Pacific Airways stocks have plunged to their lowest level in nearly a decade after the airline revealed a massive data breach has affected the information of 9.4 million passengers.

Hong Kong's flagship carrier said it had discovered unauthorised access to the personal data but had no evidence the leaked information had been misused.

Data breach documents from Hong Kong Exchanges — which operates the Hong Kong Stock Exchange — noted on Wednesday that Cathay Pacific first discovered suspicious activity on its network in March.

The documents state "unauthorised access to certain personal data was confirmed in early May 2018".

The airline noted in a statement on Wednesday that the breach was discovered during "ongoing security processes".

Cathay Pacific said the stolen data included names, nationalities, birth dates, phone numbers, addresses, passport and identity card numbers and expired credit card numbers, among other information.

It noted 403 expired credit card numbers were accessed, and 27 credit card numbers with no CVV were accessed.

The company said no passwords were compromised.

Privacy commissioner orders investigation

Hong Kong's privacy commissioner, Stephen Kai-yi Wong, expressed "serious concern" over the lapse





PHOTO: Cathay Pacific first learnt about the data breach in March. (Facebook: Cathay Pacific)

RELATED STORY: British Airways data breach affects almost 400,000 customers

RELATED STORY: 'Oops!': Cathay Pacific spells its name wrong on its own plane



Technology

Google chief says company has fired dozens of employees for sexual harassment over past two years

Refugee video game offers players glimpse of life inside detention centre

Was your favourite video game built on unpaid overtime?


TOP STORIES




- Australian shares lose another \$8b, dollar falls to 32-month low
- Six solar panels join the grid every minute, but the rush is causing problems
- Your super could be changing and now is the time to really read the fine print
- Opinion: While Gillard returns to hero's welcome, Morrison fights political fire with leaky buckets
- 'Buy a Huawei': Beijing mocks Trump after reports China and Russia are listening to his iPhone calls
- Pipe bombs were sent to his critics, but still Trump found a way to blame 'Fake News'
- Kuga was shot five times by the Taliban as he saved his mates' lives
- A town wiped out by a tsunami 25 years ago is a lesson in what not to do after disaster
- Morrison didn't tell Indigenous Affairs Minister about Abbott's new job
- This app showing people videos of them washing their own hands could help treat OCD


사례: Marriott

Secure | <https://www.wired.com/story/marriott-hack-protect-yourself/>

Revealed: Marriott's 500 Million Hack Came After A String Of Security Breaches

 **Thomas Brewster** Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.

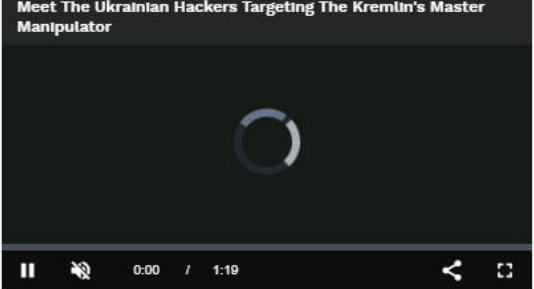






Marriott and Starwood's challenges with cybersecurity go back years, cybersecurity researchers say. AFP/GETTY IMAGES

...t Marriott revealed a massive hack led to the

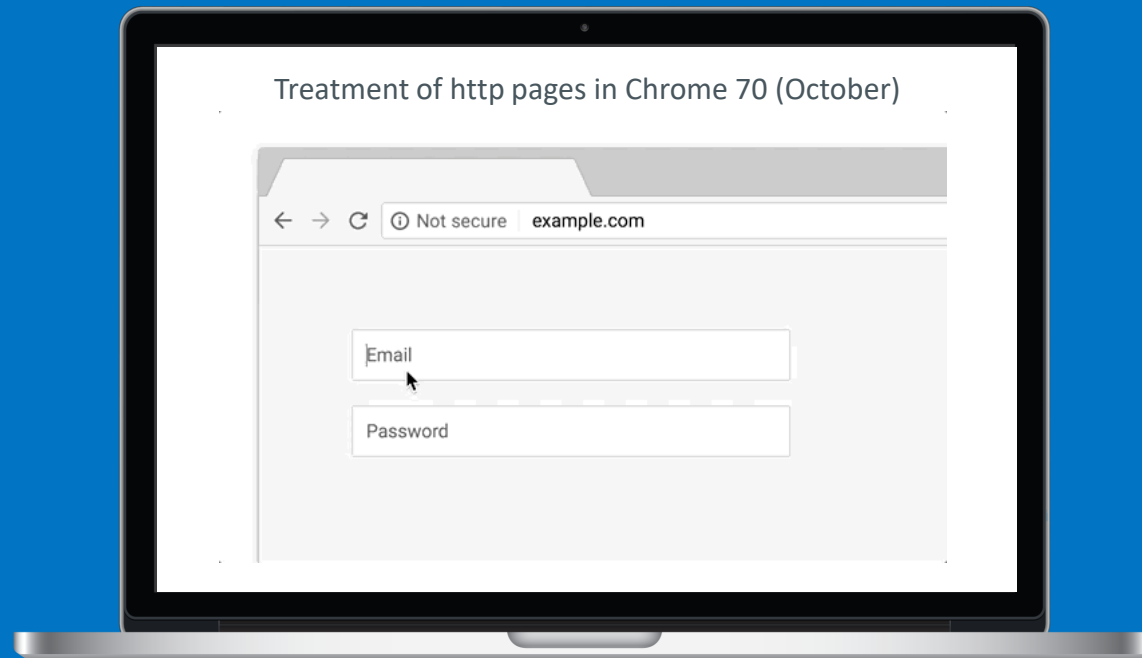
Meet The Ukrainian Hackers Targeting The Kremlin's Master Manipulator



0:00 / 1:19

“HTTPS Everywhere” 이란?

HTTPS Everywhere is simply the practice of using HTTPS across your entire website. This is in contrast to a partial deployment of SSL that may only be on certain pages—such as a log-in or check-out page. The use of HTTPS on only these “sensitive” pages was popular when the technical costs of HTTPS, such as memory overhead and CPU load, were high. Now that HTTPS has an insignificant footprint, there is no practical reason to selectively use it.



“HTTPS Everywhere”의 장점

보안 향상(Improved Security)

Implementing HTTPS across your entire site protects you and your customers from the next generation of security threats. These threats, which are described in-depth in the next section, are easy to execute. And it's not just log in credentials or credit card data that attackers are looking for—online browsing habits and personal information shared on social sites can all be used by malicious entities.



사용자 신뢰 확보

(Increased User Trust)

Because users trust SSL certificates, they are proven to increase conversion rates, improve engagement metrics, and elevate brand reputation.

According to a study by Tech-Ed, 100% of participants would prefer doing business with a company that has an EV SSL certificate. This benefit extends beyond just log in or checkout pages—by having SSL on every page of your site all of your visitors know that you are legitimate and that your identity has been verified.



브랜드 보호(Brand Protection)

Securing your users' data not only helps browsers, it helps you. Most businesses can't afford the astronomical cost of a data breach—no matter what user information is leaked. In 2017, IBM reported that companies are at an increased risk of repeated data breaches compared to last year. And, according to a 2017 Ponemon study, the average cost of a data breach is \$3.5 million.

CA/B(Certificate Authority & Browser) 포럼

CA/B 포럼 소개

- **CA(Certificate Authority) / Browser Forum**
- 인터넷 브라우저 소프트웨어 공급 업체, 운영 체제 및 기타 PKI 지원 응용 프로그램과 관련된 업계의 자발적 컨소시엄
- **X.509** 기반의 인증서 발급 및 관리를 규제하는 업계 지침을 공표
- **SSL/TLS**인증서 , **Code Sign**인증서 등 System과 Network 보안에 사용되는 인증서 지침
- SSL의 경우 **DV**(도메인 확인), **OV**(조직 유효성 검사), **EV**(확장 유효성 검사)로 분류되며 유형을 구분하기 위한 방법으로 정의



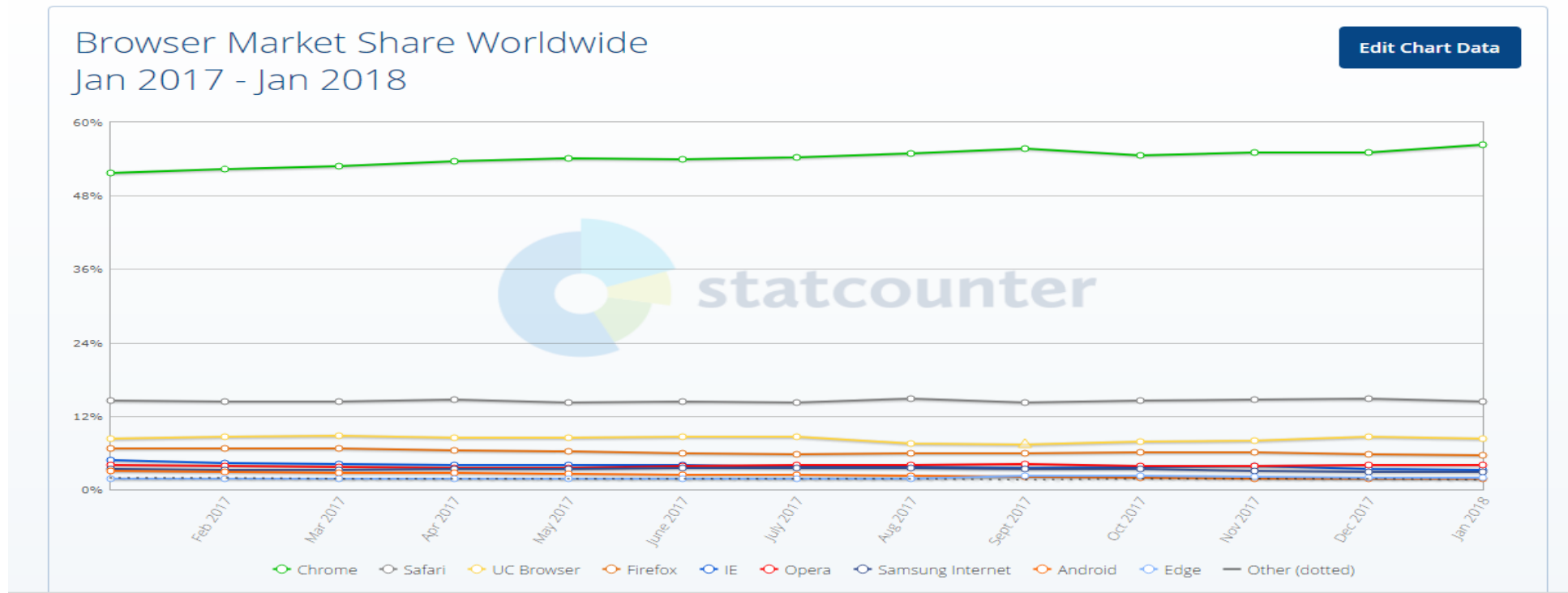
<https://cabforum.org/>

브라우저 시장 동향

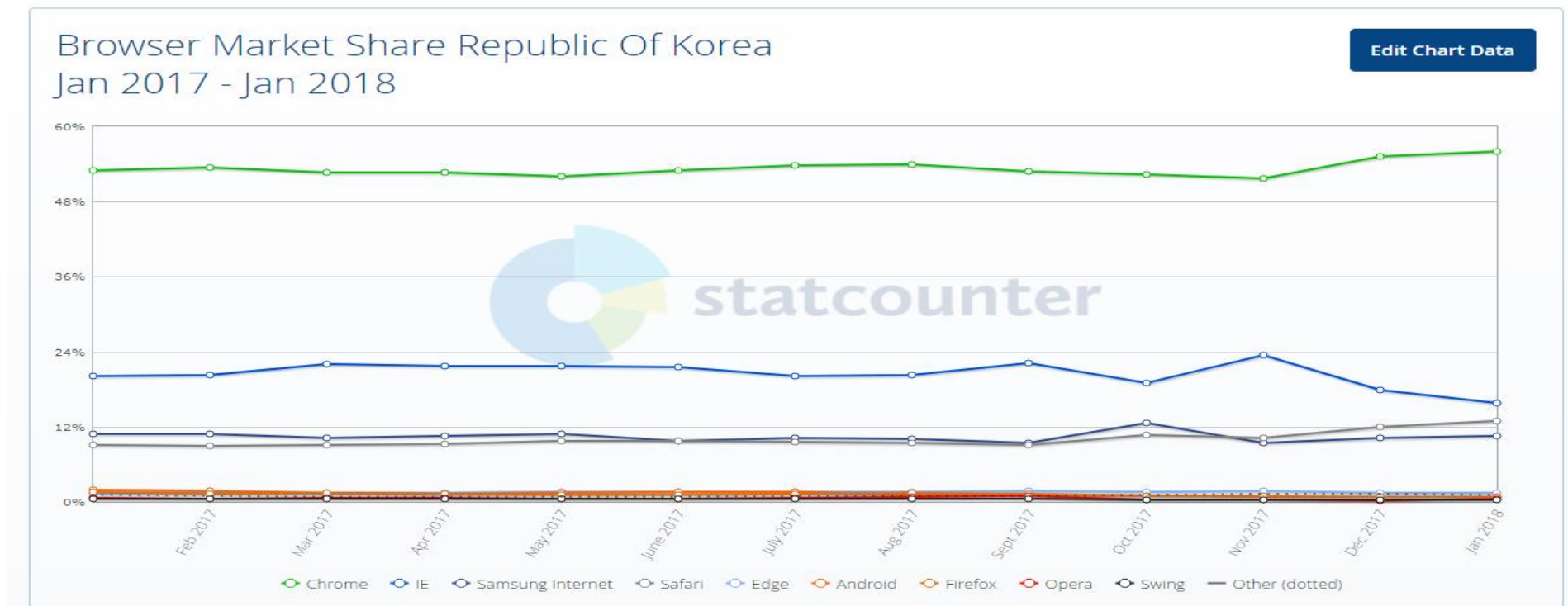
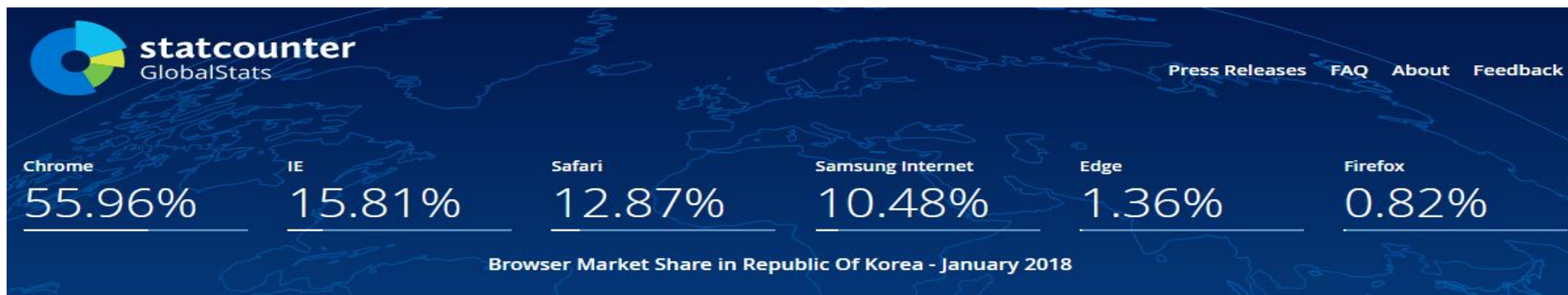
Quiz - 어떤 브라우저를?



브라우저 시장 점유율 - 전세계



브라우저 시장 점유율 - 한국



지난 해 브라우저 변화

- HTTPS가 아닌 연결에 대해 브라우저가 경고 메시지 표기
- 정부 기관의 Website는 HTTP에서 HTTPS로 전환 추세(Global 기준)
- 브라우저의 주요 기능들이 HTTPS에서만 구현 예정
- HTTP2는 HTTPS에서만 구현 가능
- Referrer Data는 HTTPS를 통해서만 가능



Browser UI treatment changes for http



>78%
of page loads in
Chrome over https



>68%
of page loads in
Android over https

Chrome의 변화

Treatment of HTTPS pages

Current (Chrome 67)

 Secure | example.com

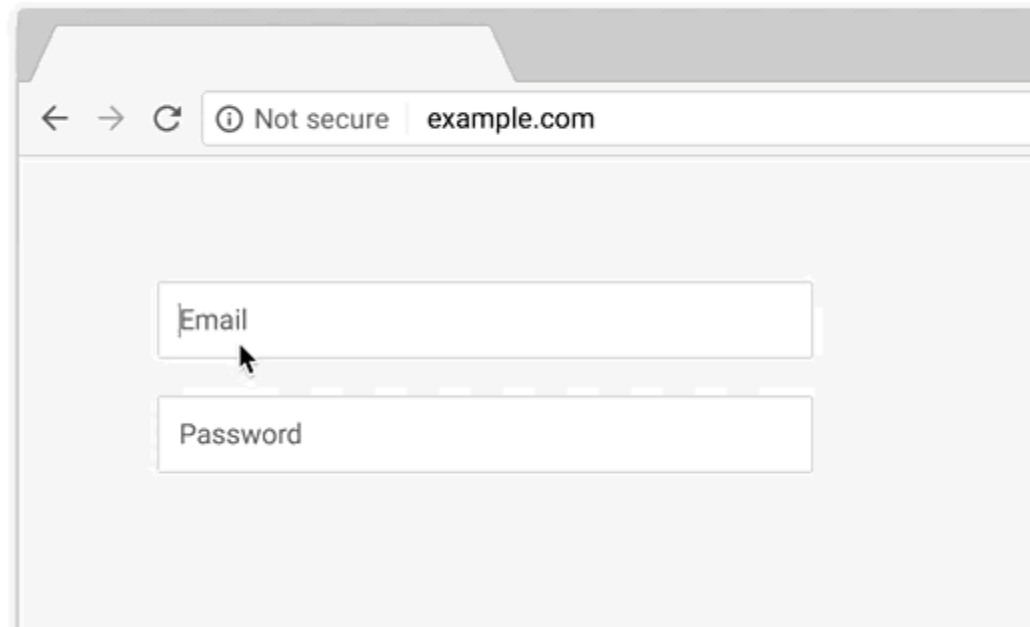
Sep. 2018 (Chrome 69)

 example.com

Eventually

example.com

Chrome 70에서의 Http에 대한 대응(2018년10월)



타 브라우저 변화



Firefox사는 HTTP에서
위치정보서비스 제공
중단(Version 55)

https://bugzilla.mozilla.org/show_bug.cgi?id=1072859




Apple사는 CT(Certificate
Transparency, 인증서
유효성) 확인 시작


<https://developer.apple.com/library/content/documentation/General/Reference/InfoPlistKeyReference/Articles/CocoaKeys.html>



Microsoft 사는 위험
Site의DV인증서에 대해
폐기 진행 예정

GPKI Chrome & Safari mobile 의 경고 문구

←  <https://m.jungleon.or.kr> 3 ⋮



연결이 비공개로 설정되어 있지 않습니다.

해커가 m.jungleon.or.kr에서 정보(예: 비밀번호, 메시지, 신용카드 등)를 도용하려고 시도 중일 수 있습니다. [자세히 알아보기](#)

NET::ERR_CERT_INVALID

[안전 페이지로 돌아가기](#)

고급

jungleon.or.kr ↻



연결된 네트워크가 비공개가 아님

이 웹 사이트는 사용자의 개인 정보 또는 금융 정보를 훔치기 위해 'm.jungleon.or.kr'(으)로 가장했을 가능성이 있습니다. 이전 페이지로 돌아가십시오.

[뒤로 이동](#)

웹 사이트의 인증서가 유효하지 않은 경우 Safari가 경고를 표시합니다. 이것은 웹 사이트의 구성이 올바르지 않거나 해커가 사용자의 네트워크 연결에 침입한 경우 발생할 수 있습니다.

더 알아보려면 [인증서 보기](#) 하십시오. 이러한 위험을 알고 있는 경우 [이 웹 사이트](#) 방문할 수 있습니다.

인증서 [완료](#)



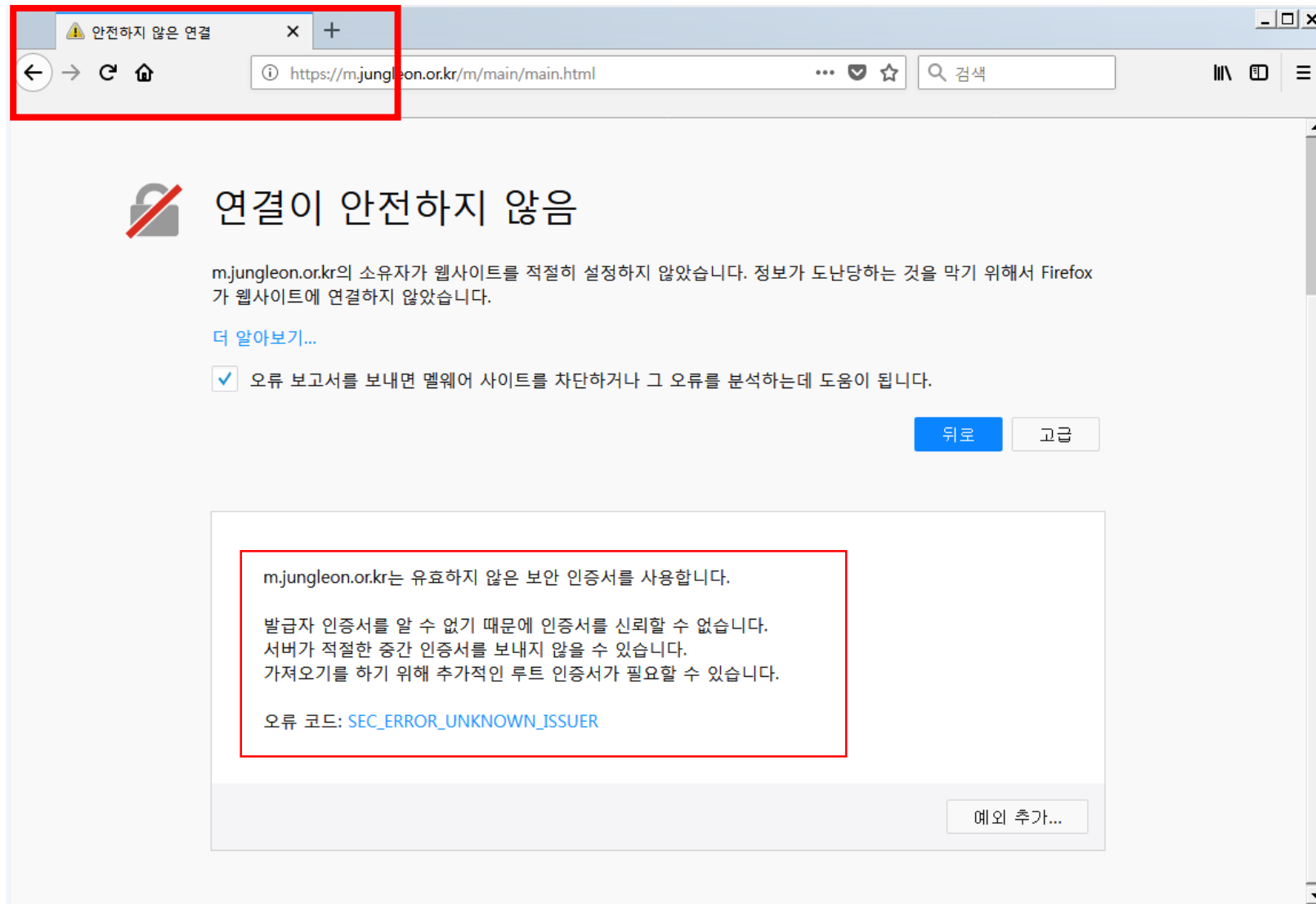
www.jungleon.or.kr
발급자 CA131100002

신뢰할 수 없음

사용 만료 2020. 2. 6. 오후 11:59:59

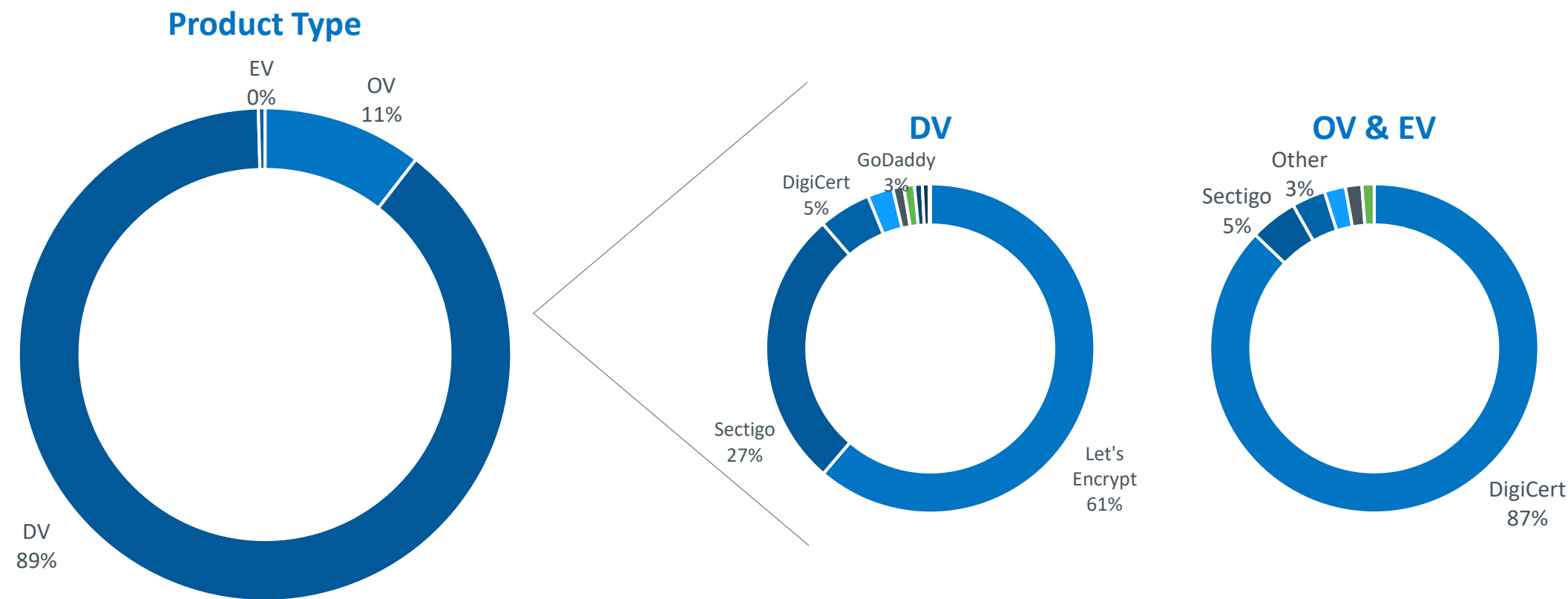
기타 세부사항 >

GPKI Firefox 의 경고 문구

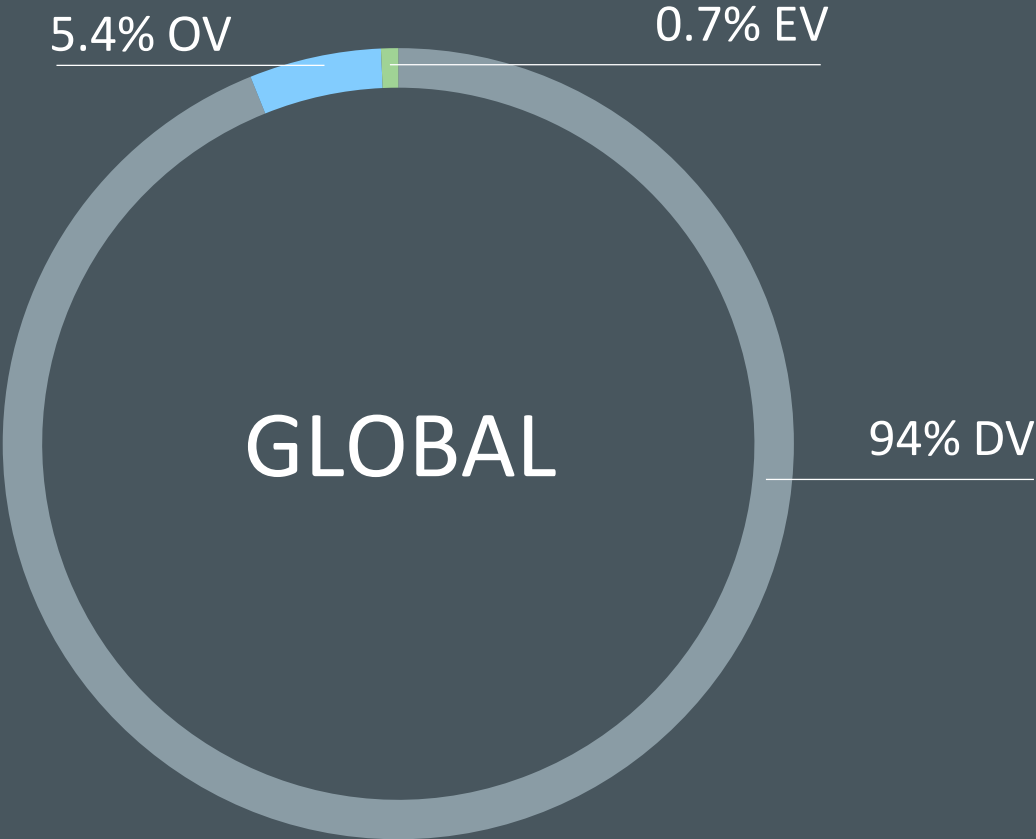


SSL 인증서 시장 동향

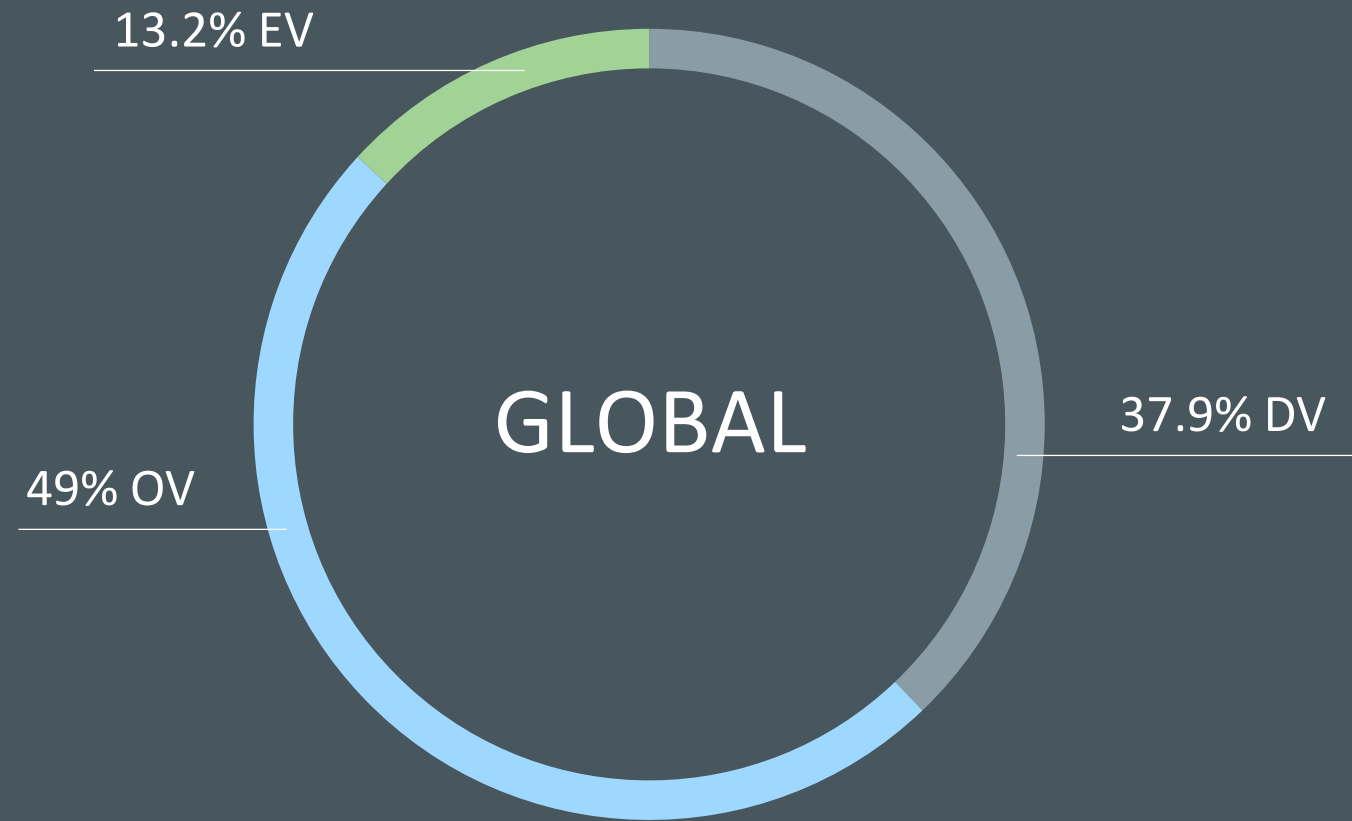
2018년12월 SSL 인증서 시장 점유율 - 전세계



인증서 종류 별 분포 - 전세계 (Breakdown of Certificate Types)

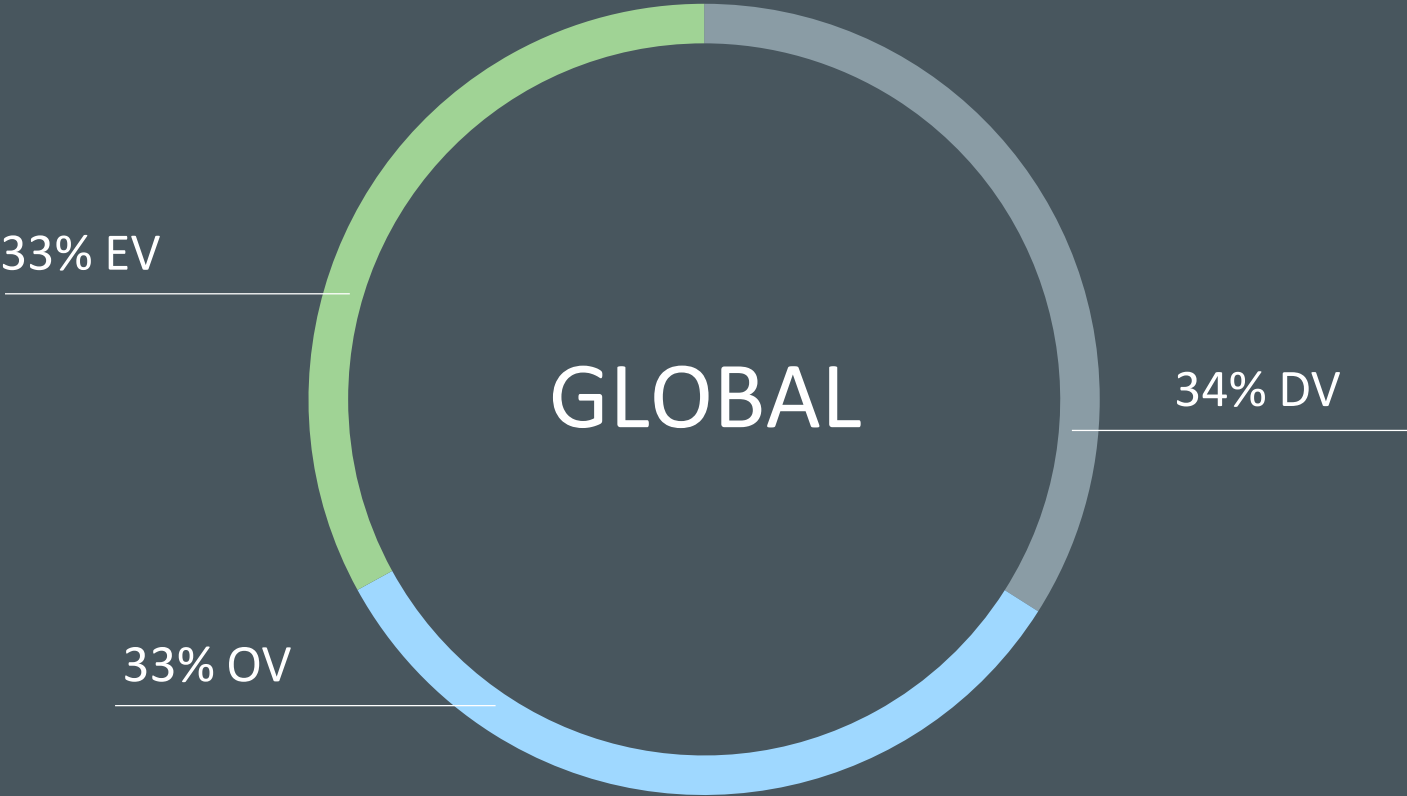


인증서 종류별 웹 트래픽 분포 – 전세계 (Share of Web Traffic by Certificate Type)



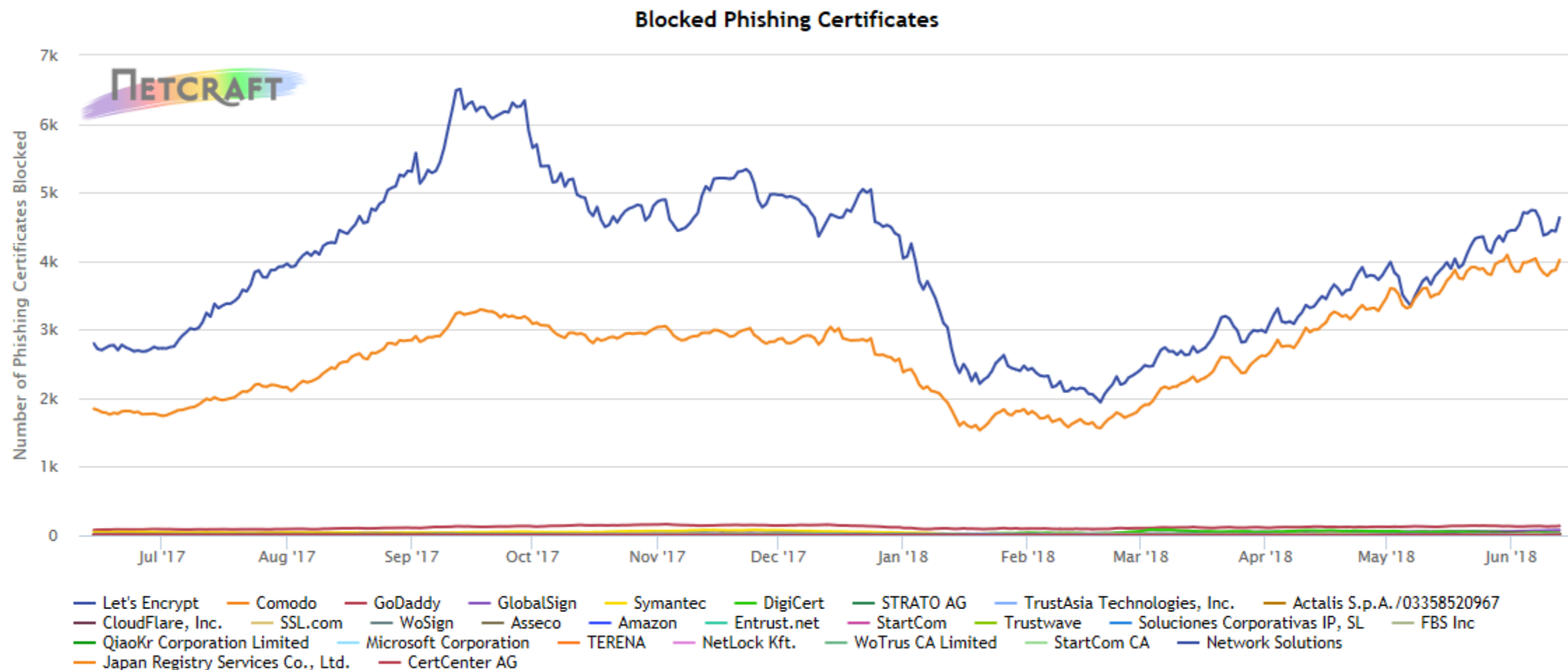
Source: Comscore and Netcraft Data, analyzed by DigiCert

인증서 종류별 상용 트랜잭션 분포 – 전세계 (Share of E-Commerce Transactions by Certificate Type)



Source: Comscore and Netcraft Data, analyzed by DigiCert

Blocked Phishing Certificates



© Netcraft 2018

EV 인증서 (Extended Validated Certificate)









tumblr.

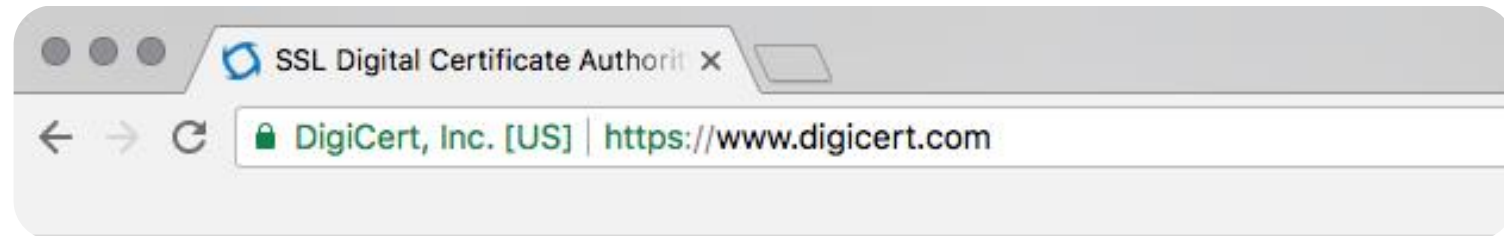
NETFLIX

WHAT IS COMMON HERE?

NETFLIX **tumblr.**



**It was all released in 2007, 12 years.
Including EV and it's standards**



EV Certificates & DigiCert



ENCRYPTION



TRADEMARK PROTECTION



BRAND RECOGNITION

DigiCert Wants to Help Improve the Process

1. Require EV certificates to specify the method of domain validation used as information in the certificate.
2. Require CAs to verify a registered trademark before issuing an EV certificate.
3. Include trademark and brand information in a certificate.
4. Provide a face-to-face verification with the certificate requester.
5. Only issue EV certificates if certain security parameters (e.g., proper Transport Layer Security (TLS) version) are met.
6. Require a valid CAA record prior to issuance.
7. Require that the CA check the certificate type in the CAA record or respect a CAA policy regarding validation processes prior to issuing.
8. Require CAs to log the identity with an identity blockchain.
9. Include LEIs in certificates.

What do you think would make EV certificates more valuable?

EV SSL 인증서 확인



IoT 동향

다양한 목적으로 사용되는 Internet

개인적 목적



BANKING



SHOPPING



LEARNING



PLAYING GAMES



COMMUNICATING



ENTERTAINMENT

업무적 목적



COMMUNICATING



TRANSACTION
PROCESSING



PRESENTING



ORDERING




RESEARCHING



HIRING

그러나, IoT 내에서는 사물은 다른 사물들과 Communication 한다

IoT (Internet of Things), 사물인터넷 이란?



The **Internet of Things (or IoT)** is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

“The installed base of **IoT endpoints** will grow from **9.7 billion in 2014** to more than 25.6 billion in 2019, hitting **30 billion in 2020.**” – IDC*

PKI & IoT 의 성장



- **25 Billion connected devices by 2020**
- 1 Billion IoT devices in Japan by 2020
- China: 27% global M2M connections
- Europe: 29%, US: 19%
- China gov. spend for M2M: USD 603B

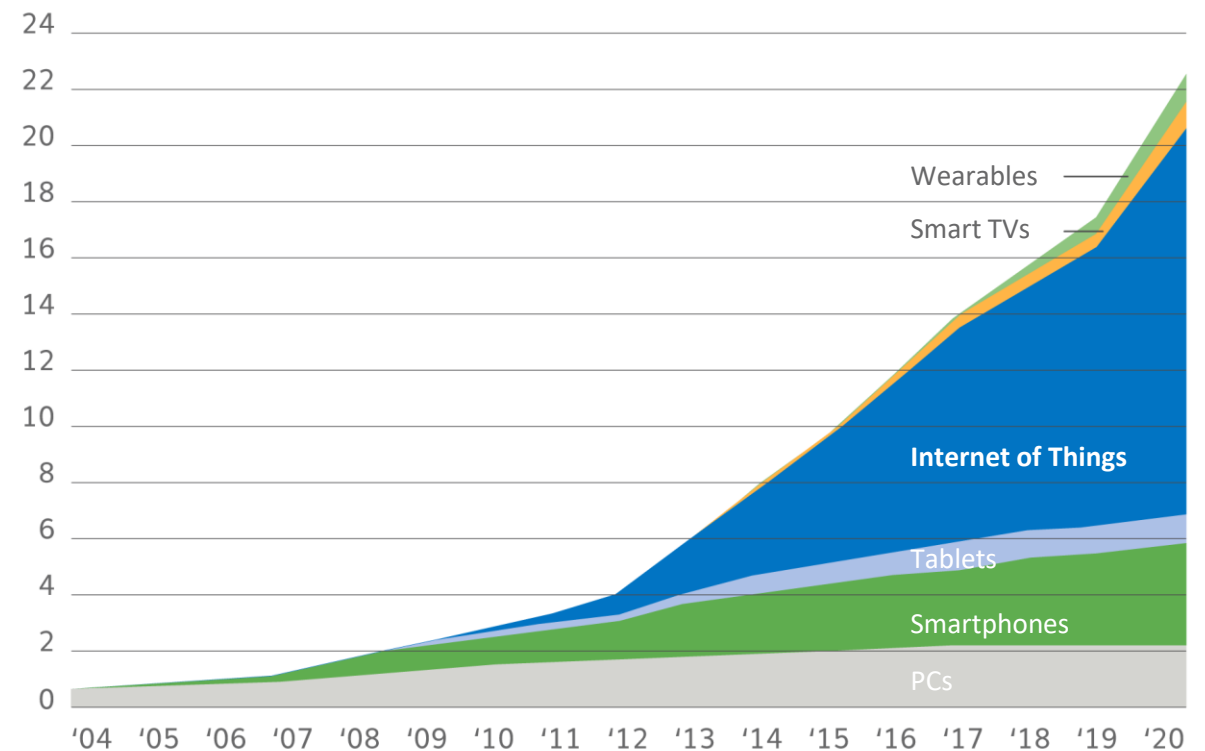


- **Global IoT Security Market (includes IAM, IPS, UTP, DLP, Analytics)**
- 2015: USD 6.89 Billion
- **2020: USD 28.9 Billion**
- **CAGR: 33.2%** from 2015–2020
- NAM: Largest market



- **Security & Privacy Concerns**
- Ubiquitous data collection
- Unintended data use

Global internet device installed base forecast



Source: Gartner, IDC, Strategy Analytics, Machina research, company filings, BII estimates

인터넷을 통해 소통하는 사물의 장점 (Benefits of *Things* communicating over the Internet)

Access to real time
information

Automatic software
updates

Remote access to
devices

Information transfer

Remote control of
devices

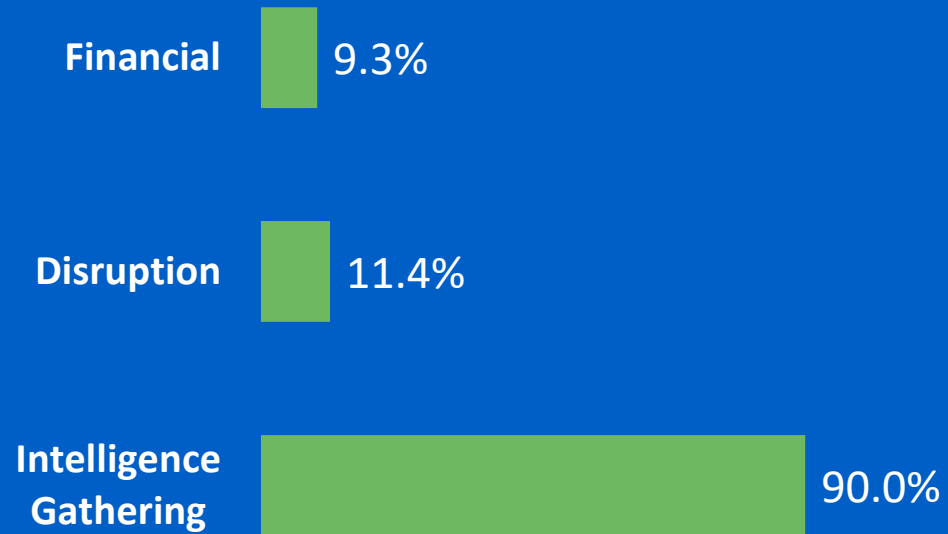
Devices can “talk” to
each other
autonomously

무슨 문제가 생길 수 있을까? (What could go wrong?)



IoT 공격 동기 - 2018 ISTR by Symantec

MOTIVES OF TARGETED ATTACK GROUPS



TOP 10 COUNTRIES AFFECTED BY TARGETED ATTACKS

Rank	Country	Total
1	U.S.	303
2	India	133
3	Japan	87
4	Taiwan	59
5	Ukraine	49
6	South Korea	45
7	Brunei	34
8	Russia	32
9	Vietnam	29
10	Pakistan	22

왜 IoT device가 보안에 취약한가? (Why are IoT devices insecure?)

- Manufacturers lack cybersecurity experience (and security is hard!)
- Costs to secure can be prohibitive
- Personal devices are designed to be easy to use, sacrificing security
- Cybersecurity sometimes sacrificed for expediency
- Competing standards can be difficult to navigate – creating security “blind spots”
- For many consumer devices, time to market and cost rule over security
- Some devices use factory default passwords
- Inability to apply patches for security
- No or weak encryption
- Lack of penetration testing and vulnerability analysis before deployment
- Unprotected APIs
- Leaking of private data

IoT device를 위한 기초 보안 (Basic Security for IoT Devices)

Avoid direct Internet
connection

Check defaults

Change default
credentials

Avoid P2P connections

Update the firmware

Consider cost

인증서는 IoT device 보안을 위해 어떤 역할을 하는가?

(How Certificates Play a Role in Securing IoT devices)



Strong authentication of
the device



Enable encryption
between end points



Digital signing of code
used in IoT devices

IoT 보안 적용 사례: www.digicert.com/blog

회사 소개 – DigiCert

DigiCert – SSL인증서와 IoT 보안 선도 기업

- 높은 신뢰도를 보장하는 **SSL, PKI, & IoT solutions*** 선도 업체
- 웹사이트와 IoT를 위한 신원확인, 인증, 암호화 솔루션 제공
- **매일 260억 개 Web connection**의 안전한 연결 보장
- Global 2000의 **83%**와 Top global banks의 **97%**가 선호
- 2017년 10월 Symantec SSL 사업부문 인수를 통해 업계 최정상의 기술력 확보를 통하여 보다 간편한 SSL, PKI & IoT 솔루션 제공
- 2018년 10월 **DigiCert-Gemalto-Isara** 등 3사가 **양자 컴퓨팅** 시대의 미래 사물인터넷(IoT) 보안을 위한 파트너십 체결
- 2019년 1월 **Quo Vadis CA** 인수

#1
SSL Provider
FOR ENTERPRISE


180+
COUNTRIES SERVED


1,000+
EMPLOYEES


24/7/365
CUSTOMER SUPPORT



Offices: Lehi, Utah; St. George, Utah; Tokyo, Japan; Mountain View, California; Cape Town, South Africa; Dublin, Ireland; Melbourne, Australia; Pune, India & many others

*according to Netcraft and 451 Group analysis.

A Combined History of Innovation & Leadership

1995

VeriSign becomes the first Certificate Authority



2003

DigiCert founded based on the question, "Isn't there a better way?"

digicert®

2007

DigiCert partners with Microsoft to develop first Multi-Domain certificate



2013

DigiCert builds first CT log accepted by Google



2016

DigiCert acquires Verizon SSL/TLS business



2018

DigiCert's trusted roots become encryption foundation for enterprises worldwide



1997

VeriSign becomes first international CA



2005

DigiCert becomes founding member of the CA/Browser Forum



2010

Symantec acquires Verisign Authentication



2015

DigiCert launches scalable IoT platform



2017

DigiCert acquires Symantec's Website Security business



2019

DigiCert acquires QuoVadis CA

QuoVadis

(주)파인앤서비스("CertKorea")

웹사이트 개인정보보호를 위한 SSL 인증 솔루션 리더

- 2000년부터 SSL 솔루션을 국내에 도입한 보안/인증 업계 리더
- 높은 업력으로 19년째 국내 10,000여개 고객 레퍼런스 보유
- 국내 유수 기업에 4만 건 이상 SSL 인증서비스를 제공
- 세계 최대 인증기관 디지서트(DigiCert) 플래티넘 파트너 사로 선정
디지서트(DigiCert) 로부터 하이퀄리티의 기술 지원과 마케팅 지원 받음
- 대기업 및 금융권, 정부기관 등 국내 유수 기업으로 부터 높은 신뢰를 받음
- 우수한 고객서비스와 24시간 / 365일 연중무휴 기술 지원 서비스를 제공

주요 고객사 * 국내 10,000여개 고객사

 통계청	 KSD 한국예탁결제원	 KRX 한국거래소 KOREA EXCHANGE	 UX 한국국토정보공사 Korea Land and Geospatial Information Corporation	 금융보안원 FINANCIAL SECURITY INSTITUTE
 SAMSUNG	 LG U+	 DOOSAN	 Hanwha	 kakao
 kakaobank	 KB 국민은행	 신한은행	 하나은행	 IBK 기업은행

2018



DigiCert 웹시큐리티
플래티넘 파트너
선정

2012

GeoTrust Inc. 파트너 제휴 체결



2005

KISA

한국인터넷진흥원
보안서버협의회 회원사 등록
KISA 인증서비스 제공

2002

세계1위 인증기관
Verisign Inc. 파트너 제휴
체결
Thawte Inc.
파트너 제휴 체결



2000

- 첨단 부설연구소 인가
- KAIST첨단기술사업화센터 (HTC) 입주기업
- 정보통신부 장관상 (우수IP상 수상)



감사합니다.

DigiCert Ireland Limited, Korea Branch

나 정주 지사장

(Country Manager for Korea, Indonesia, Pakistan and Vietnam)

James.Nah@digicert.com

(주)파인앤서비스

허 명옥 총괄팀장

cert@certkorea.co.kr