Who am I Talking To?
Ambiguities in secure certificates for web commerce

(Preliminary)

John Nagle
SiteTruth
November, 2014

Introduction

At SiteTruth, our business is finding the real-world business behind a web site and checking its legitimacy and reputation. Secure certificates are one source of information. We thus have an interest in the fields in a secure certificate which identify business organizations.

According to the CA/Browser Forum, there are three types of Secure Sockets Layer certificates.

- Domain Validation (DV) - A Domain Validated SSL certificate is issued after proof that the owner has the right to use their domain is established. “Minimal checks” are performed.
- Organizational Validation (OV) - Certification authorities must validate the company name, domain name and other information through the use of public databases. The certificate contains the company name and the domain name for which the certificate was issued for. This is the minimum certificate recommended for ecommerce transactions.
- Extended Validation (EV) - EV Certificates are only issued once an entity passes a strict authentication procedure. These checks are much more stringent than OV certificates.

We are concerned with the accuracy of business information in OV and EV certificates. Here, we look at certificates which certify more than one domain name.

Multi-domain certificates

SSL certificates which contain multiple second-level domains are used for several purposes. Multiple brands or business units of a single business may be consolidated under one certificate. This is clearly legitimate. However, there is also a practice of using “shared SSL certificates”, where a number of domains appear on a single SSL certificate issued by a certification authority. These are typically used by hosting services and front-end intermediary services caching data for performance or protecting sites against attacks.

Front-end services use certificates in this way because of a legacy problem. With Server Name Indication protocol as part of Transport Layer Security, sharing of certificates is no longer necessary, even when IP addresses are shared. All major browsers have supported this since 2007. It is supported in Internet Explorer 7 and later, Safari 3.0 or later, Google Chrome 6 or later, and Firefox 2.0 or later.

Windows XP and Internet Explorer 6 do not understand Server Name Indication protocol. Windows XP sales ceased in 2008, and in 2014 Microsoft terminated support for Windows XP, but it still has 17% browser market share as of October 2014. It is the desire to support these legacy systems which creates a technical need for shared SSL certificates.

As a result, there exist many certificates which have Organization information in the certificate which identifies an intermediary service instead of the actual destination. In this paper, we take a close look at such certificates.

Methodology

We examined all SSL certificates visible on the web in IPv4 address space. The Zmap project at the University of Michigan collects such certificates by scanning all IPv4 Internet addresses and makes the data available.[1] The data set used here is the set of February 5, 2014. It contains 66,335,624 certificates, of which 4,771,739 contain domain names from more than one second level domain.

The definition of a "second level domain" used is based on the Public Suffix List established by the Mozilla Foundation.[2] It represents the part of a domain name which is **not** under the control of the individual registrant. Because of the existence of suffixes such as ".co.uk", determining what is a secon-level domain is non-trivial. Domains registered through an ICANN-approved registrar normally comprise a customer-chosen second level domain followed by a public suffix. Such domains are purchased by an individual or business entity, and are thus the level at which a business entity is attached to a domain.

Determining whether a certificate is DV, OV, or EV is established by examining the Certificate Policies extension of each certificate. Certificate Policies are identified by Object Identifiers (OIDs), which are strings composed of numbers separated by dots. (These have no connection to Internet addresses.) The CA/Browser Forum has established generic OIDs for DV, OV, and EV certificates. However, Certificate Authorities are not required to use these values. Each Certificate Authority can choose values of their own and publish them in their Certification Practice Statement. We have examined all the Certification Practice Statements of the members of the CA/Browser Forum and constructed a list.[3] **As of this writing, the list is incomplete due to translation problems, but the OIDs for all the major non-China CAs have been listed.**

Self-signed certificates, and ones not accepted by a major web browser, have been excluded.

Results

Top 25 organizations named in CA-issued, browser-valid certificates associated with large numbers of domains.

1 "Analysis of the HTTPS Certificate Ecosystem", by Zakir Durumeric et al, Department of Electrical Engineering and Computer Science, University of Michigan, 2013. Proc. 13th Internet Measurement Conference (IMC '13)

2 Public Suffix List, from "publicsuffix.org".

3 CA OID Table, "https://github.com/John-Nagle/certscan/blob/master/data/catypetable.ods"

Common Name	Organization	Certification Authority	Type	Domains
cloudflare.com	CloudFlare, Inc.	GlobalSign Organization Validation CA - G2	OV	36280
incapsula.com	Incapsula Inc	GlobalSign Organization Validation CA - G2	OV	1471
sonymusic.com	Sony Music Entertainment	COMODO High-Assurance Secure Server C	DV	999
bosch-bayileri.com	www.bosch-bayileri.com	Go Daddy Secure Certification Authority	DV	874
janrainengage.com	JanRain, Inc.	DigiCert High Assurance CA-3	OV	678
edgecastcdn.net	EdgeCast Networks, Inc.	DigiCert High Assurance CA-3	OV	625
sonymusic.com	Sony Music Entertainment	COMODO High-Assurance Secure Server C	OV	601
fiducia.de	Fiducia IT AG	COMODO High-Assurance Secure Server C	DV	599
fiducia.de	Fiducia IT AG	COMODO High-Assurance Secure Server C	OV	599
vin65.com	K1 Technology Corp	DigiCert High Assurance CA-3	OV	588
practiceweb.co.uk	PracticeWEB Limited	GlobalSign Organization Validation CA - G2	OV	577
sonymusic.com	MyPlayDirect Inc.	COMODO High-Assurance Secure Server C	DV	488
sonymusic.com	MyPlayDirect Inc.	COMODO High-Assurance Secure Server C	OV	488
indiebound.org	American Booksellers Associ	DigiCert High Assurance CA-3	OV	462
patriotwebmarketing.c	Patriot Web Marketing, LLC	DigiCert High Assurance CA-3	OV	458
vtexcommerce.com.b	Vtex Informatica S.A.	DigiCert High Assurance CA-3	OV	452
vin65.com	K1 Technology Corp DBA Vin	DigiCert High Assurance CA-3	OV	448
palmwebservices.com	Palm Web Services, LLC	DigiCert High Assurance CA-3	OV	435
cdnetworks.net	CDNetworks Inc.	DigiCert High Assurance CA-3	OV	364
profilo-bayileri.com	www.profilo-bayileri.com	Go Daddy Secure Certification Authority	DV	364
cdngc.net	CDNetworks Inc.	DigiCert High Assurance CA-3	OV	342
lithium.com	Lithium Technologies, Inc.	DigiCert High Assurance CA-3	OV	313
NONE	Uniform Market LLC	COMODO High-Assurance Secure Server C	DV	312
NONE	Intelligent Retail Ltd	COMODO High-Assurance Secure Server C	DV	310
acquia-sites.com	Acquia Inc.	DigiCert High Assurance CA-3	OV	278

Note that many of the multi-domain sites listed have their domains listed as Organization Validated. These are the ones of greatest concern. These are organizations which have a very large number of unrelated domain names tied to one organization.

Certificates naming many unrelated domains

The list above allows us to identify the major players for which the certificates are listed as "Organization Validated", but domain name and the organization behind the domain are not related. The top few sites are:

- cloudflare.com – a front-end network for sites, controlling 36,280 domains.
- incapsula.com – a front-end network for sites
- sonymusic.com – operates sites for their range of artists.
- Janrainengage.com – customer tracking service
- edgecastcdn.net – Verizon caching system
- fiducia.de – security service for banks
- vin65.com – wine seller with many sites for various wine brands.
- practiceweb.co.uk – a hosting service for accountants

Other than the music and wine sellers, each of these is an intermediary network service which acts on

behalf of some other organization. Each of these services terminates the SSL connection at their own servers, acting as a man-in-the-middle, and then passes the data on to the actual web server for the business using the site.[4]

The certificates presented by these intermediary network services identify the network service, not the ultimate destination site. Cloudflare, Inc. has 36,280 domains tied to “cloudflare.com”, all with OV certficates. The Organization field in these certificates is”Cloudflare, Inc”, not the business which owns the web site behind the domain. This is the problem.

Extended validation certificates naming many unrelated domains

There aren't any. Standards are higher at the EV level.

4 We will pass over the security, privacy, and legality of this arrangement at this time.

Top 25 organizations named in CA-issued, browser-valid Extended Validation certificates associated with large numbers of domains.

Common name	Organization	Certification Authority	Type	Domains
coolblue.be	Coolblue NV	COMODO Extended Validation Secure	EV	121
coolblue.nl	Coolblue BV	COMODO Extended Validation Secure	EV	119
tellsubway.com	Doctor's Associates Inc./2	Entrust Certification Authority - L1E	EV	76
tellsubway.com	Doctor's Associates Inc./I	Entrust Certification Authority - L1E	EV	76
jardenstore.com	Jarden Corporation	VeriSign Class 3 Extended Validation	EV	63
tellsubway.tt	Doctor's Associates Inc./2	Entrust Certification Authority - L1E	EV	62
NONE	Eni S.p.A.	Actalis Authentication CA G2	EV	59
NONE	Holiday Extras Ltd	COMODO Extended Validation Secure	EV	59
sued-west.com	Sued-West Versand Gmb	GlobalSign Extended Validation CA - (	EV	58
skelters.nl	XLShop Group B.V.	COMODO Extended Validation Secure	EV	49
paypal.co.uk	PayPal, Inc.	VeriSign Class 3 Extended Validation	EV	44
NONE	Totalstay LTD	COMODO Extended Validation Secure	EV	39
thefa.com	The Football Association	QuoVadis Global SSL ICA	EV	39
bmo.com	Bank of Montreal/2.5.4.15	Entrust Certification Authority - L1E	EV	37
sundiogroup.com	Sundio Group B.V.	GlobalSign Extended Validation CA - (	EV	36
marykay.com	Mary Kay, Inc.	COMODO Extended Validation Secure	EV	35
paypal.co.uk	PayPal Pte Ltd	VeriSign Class 3 Extended Validation	EV	35
sundiogroup.com	Rotterdam Leisure Holdin(	GlobalSign Extended Validation CA - (	EV	34
bmo.com	Bank of Montreal/2.5.4.15	Entrust Certification Authority - L1E	EV	33
coke.com	The Coca-Cola Company	Trend Micro CA	EV	32
apartments4you.com	Wyndham Worldwide Corp	VeriSign Class 3 Extended Validation	EV	31
eurocampings.nl	ACSI Publishing B.V.	COMODO Extended Validation Secure	EV	30
mister-auto.com	MISTER AUTO SAS	GlobalSign Extended Validation CA - (	EV	29
villeroy-boch.com	Villeroy & Boch AG	COMODO Extended Validation Secure	EV	29

None of these are front-end network services. They are all large companies which operate across multiple countries, languages, and brands. The number of domains per organization is modest.

- coolblue.be and coolblue.nl – a retailer with many product lines, each with its own site clearly identified as Cool Blue
- tellsubway.com – Subway, the fast-food company, is a subsidiary of Doctor's Associates, Inc. and has a large number of sites in different countries and languages.

Organization ambiguity is not a problem at the EV level.

Solutions

We would like to have some information item in certificates which indicates the certificate does not represent the owner of the domain, but rather some proxy, hosting service, or intermediary. Failing that, the issuance of OV certificates for such organizations may be inappropriate. The CA/Browser Forum's standard in this area, the Baseline Requirements[5], does not address the issue where the “subject” of the certificate is an intermediary service, not the ultimate destination of the connection. This ambiguity creates problems. This ambiguity should be cleared up, and it should be made clear, via information in

5 CA/Browser Forum Baseline Guidelines, version 1.2,3, October 2014, at https://cabforum.org/wp-content/uploads/BRv1.2.3.pdf

certificates when an intermediary is involved.

As an interim solution, we are creating a blacklist of services which present non-useful organization information in OV certificates. This blacklist will contain about 20 such services. For sites on the blacklist, OV certificates will be treated as DV certificates and given no weight in SiteTruth rankings.

Conclusion

The Organization field in OV certificates cannot be taken as reliably indicating the organization with which the client is dealing. Workarounds are necessary to detect and reject the information in certain certificates. Pending a more permanent solution, a short blacklist is sufficient to deal with the problem.

Appendix 1 – Data analysis tools

The primary data file used for this analysis is

`https://scans.io/data/umich/https/certificates/certificates.csv.gz`

The program used to analyze this data is at

`https://github.com/John-Nagle/certscan`

The “certscan” program extracts certificates containing multiple second-level domains from the full file of all certificates, and loads them into a MySQL database for further analysis. The tables in this paper were generated from that database.