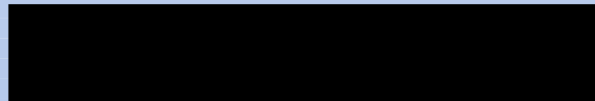


# TLS trends at GCHQ



# Source of data

- Our TLS events come from our TLS app
  - Runs on special source (approx. 200 x 10G) and Comsat data
  - Produces unselected events: about 10 billion Server Hellos per week
- Records details about the handshake: IPs, Hello messages, Certificate, Key Exchanges
- Events stored for 6 months in our clouds

# Trends Reports

- We summarise these events to produce weekly trends reports, which record:
  - Types of key exchange (RSA/DH/EC)
  - “Top 40” TLS services in use, highlighting new services and changes in existing services
  - Details about the crypt (e.g. DH moduli)
  - “Watchlist” to keep an eye on widely-used services (Facebook, Gmail, Hotmail, etc)

# Example: top 40 services

#1 Top Certificates seen by Common Name

Common Name	Modulus	valid from	valid until	Issuer org	Position	% of Total	Past %	Raw Count
*.facebook.com	BDAF38FB408B8B337B1D... (1024)	13/01/10	11/04/13	DigiCert Inc	1 (1)	9.291 (10.205)	=====	968772690 (1127419008)
a248.e.akamai.net	B40134F190AE8E48066F... (1024)	01/09/11	31/08/12	GTE Corporation	2 (2)	7.695 (7.046)	=====	802295227 (778458790)
www.facebook.com	B87B00B4783DF3CB4611... (1024)	17/11/11	13/07/12	VeriSign Trust Network	3 (3)	5.096 (5.443)	=====	531368555 (601326037)
api.twitter.com	D8ABCC50A9C36696D9AB... (2048)	18/05/10	17/05/12	VeriSign, Inc.	4 (4)	4.440 (4.839)	=====	463021773 (534657717)
*.hotmail.com	956F4C1D7B4904F9CAA6... (2048)	13/07/11	12/07/13		5 (5)	2.728 (2.624)	=====	284430903 (289947972)
urs.microsoft.com	A7182FC26B834C47BFC... (1024)	16/05/11	15/05/12		6 (6)	2.656 (2.584)	=====	276995437 (285510909)
*.channel.facebook.com	C5386D6248B91DE99A04... (1024)	23/11/10	26/11/13	DigiCert Inc	7 (7)	2.242 (2.401)	=====	233793675 (265316019)
s-static.ak.fbcdn.net	C8E627515E97A92B68EE... (1024)	01/08/11	01/08/12	Akamai Technologies Inc	8 (10)	2.180 (1.584)	=>=====	227382435 (175019929)
m.facebook.com	D10FC5EBFC66EB82D938... (1024)	29/05/11	01/06/13	Equifax	9 (14)	2.046 (1.520)	=>=====	213407210 (167941977)
*.data.toolbar.yahoo.com	AF227F382DE62FFA45EE... (1024)	24/06/10	25/08/13	Equifax	10 (11)	1.737 (1.573)	=====	181117743 (173876822)
login.yahoo.com	B4F12A8383CD3CD6CCE... (1024)	21/12/10	03/01/13	DigiCert Inc	11 (17)	1.719 (1.409)	=====	179230294 (155713115)
*.icloud.com	B9053E899228403B6457... (2048)	02/06/11	02/08/13	Entrust, Inc.	12 (9)	1.714 (1.753)	=====	178784944 (193662902)
*.google.com	A9619B9519E2AF788A45... (1024)	08/03/12	08/03/13	Google Inc	13 (12)	1.478 (1.542)	=>>=====	154111639 (170445646)
www.update.microsoft.com	AC563853D7E933BD71F7... (2048)	19/04/11	18/04/13		14 (15)	1.296 (1.466)	=====	135141462 (161960265)
s-static.ak.facebook.com	A058EA4811BD70EDFC21... (1024)	29/07/11	29/07/12	Akamai Technologies Inc	15 (18)	1.252 (1.354)	=====	130543626 (149630545)
api.login.icq.net	C4B160ABD2B025383DF4... (2048)	30/06/11	16/08/17	VeriSign, Inc.	16 (35)	1.188 (0.478)	>>>>>=====	123931507 (52863604)
imap.gmail.com	9AFDA9BEF8573E238052... (1024)	18/11/11	18/11/12	Google Inc	17 (25)	1.160 (0.659)	>>>>>=====	120963041 (72889992)
login.live.com	C54803D383594EAC8B19... (2048)	28/09/11	27/09/12	VeriSign, Inc.	18 (21)	1.094 (0.960)	=====	114138558 (106107395)
pop3.live.com	A906AEC8EB6826C51BE... (2048)	24/03/11	23/03/13		19 (20)	1.048 (1.024)	=====	109361276 (113150224)
twitter.com	9A21AA930F40AE99EFBD... (2048)	07/07/11	27/07/12	VeriSign, Inc.	20 (19)	0.969 (1.128)	=====	101088158 (124647248)
http.mws.mobile.live.com	F8B16F57A4599C6F346F... (1024)	12/08/10	30/09/14	VeriSign Trust Network	21 (16)	0.955 (1.450)	=>>><=====	99584853 (160275556)
*.ak.fbcdn.net	AB42786DB7E50E2EFEBF... (1024)	13/01/12	13/01/13	Akamai Technologies Inc	22 (22)	0.931 (0.907)	=====	97155933 (100210124)
*.facebook.com	AE94B171E2DECC1693E... (1024)	14/07/11	13/07/12	VeriSign Trust Network	23 (13)	0.843 (1.525)	=====	87967311 (168474280)
*.imap.mail.yahoo.com	D4EBE5BEC7F392CC63E2... (2048)	11/05/11	15/05/13	DigiCert Inc	24 (29)	0.702 (0.584)	=====	73246541 (64522656)
*.itunes.apple.com	BE929951748692E0F512... (1024)	23/06/09	22/06/14	VeriSign, Inc.	25 (23)	0.688 (0.739)	=====	71781445 (81745924)
TrustedSourceServer_IMQAO1	DAB6EBE776DCFBD330B... (1024)	18/02/10	01/01/38	SCC	26 (28)	0.669 (0.614)	=====	69784882 (67857652)
www.google.com	DEB72643A69985CD38A7... (1024)	26/10/11	30/09/13	Thawte Consulting (Pty) Ltd.	27 (24)	0.665 (0.738)	=====	69403948 (81563480)
*.whatsapp.net	DA6040129F6D3C9ACB3D... (2048)	31/12/09	31/12/12	GoDaddy.com, Inc.	28 (27)	0.627 (0.627)	=====	65465951 (69350595)
games.metaservices.microsoft.com	C830F15AD53CE2589378... (2048)	16/05/11	15/05/13		29 (26)	0.606 (0.630)	=====	63213853 (69606626)
*.cityville.zynga.com	D5A3EE989786818E9EC2... (2048)	29/06/11	28/06/12	VeriSign, Inc.	30 (37)	0.583 (0.451)	=====	60885889 (49891238)
*.zynga.com	CF2A2823980A14D7009F... (1024)	01/09/11	30/12/13	DigiCert Inc	31 (33)	0.569 (0.521)	=====	59409296 (57599432)
*.twitter.com	ACBDEF362314A01E035E... (2048)	17/07/11	17/09/13	GeoTrust, Inc.	32 (30)	0.554 (0.575)	=====	57778165 (68623577)
*.mail.ru	AFD70CA3E329E37E15A6... (2048)	12/03/12	11/05/14	Thawte, Inc.	33 (42)	0.530 (0.425)	=>=====	55267751 (48962081)
contacts.msn.com	965A1B80EBB656C1D69E... (2048)	12/05/11	11/05/13		34 (34)	0.514 (0.506)	=====	53694286 (55968833)
*.s3.amazonaws.com	93CD135CD0BD05608C... (1024)	15/12/10	18/12/13	DigiCert Inc	35 (38)	0.509 (0.450)	=====	53084116 (49720339)
*.addons.mozilla.org	B612D697D0571AFE9153... (2048)	27/12/10	29/12/12	GeoTrust, Inc.	36 (31)	0.492 (0.550)	=====	51395280 (60762021)
*.securestudies.com	DC1591DB0B316C39526B... (2048)	02/03/12	19/03/13	COMODO CA Limited	37 (82)	0.470 (0.143)	>=====	49056755 (15851007)
sb01.cysheiev.htit.prd.miyowa.net	D78B03F0D9C9E8B94415... (2048)	19/04/11	20/04/13	The USERTRUST Network	38 (39)	0.444 (0.447)	=====	46338349 (49394988)
*.castle.zynga.com	DA8920606F8929E98631... (1024)	01/09/11	30/12/13	DigiCert Inc	39 (44)	0.438 (0.396)	=====	45721029 (43761752)
gs-loc.apple.com	CC785DBDA5E720FE810B... (2048)	04/10/10	01/10/12	Entrust, Inc.	40 (43)	0.419 (0.421)	=====	43766504 (46590125)
*.calendar.yahoo.com	C024E5101CA04AA804F7... (2048)	13/03/12	20/03/13	DigiCert Inc	41 (63)	0.405 (0.205)	>>=====	42323610 (22677002)

# Trends Reports: Findings

- RSA:DH:EC ratio roughly constant (90:5:5)
  - \_ EC almost entirely Google (plus a bit of whatsapp)
- New certificates mostly use 2048-bit RSA keys
- We've seen new services jump up the list:
  - \_ Summer 2011: Google's switch to Elliptic Curves
  - \_ Autumn 2011: Apple's iCloud service
  - \_ Spring 2012: Increase in mobile Facebook encryption

# TLS and targets

- Trends reports not based on targeted data
- How do we judge interest in TLS services, and get analysts involved? Two ways we've tried:
  - Associate TLS events with targets, and inform the relevant analysts (TargetTLS)
  - Put TLS data out there for analysts to search (FLYING PIG)

# TargetTLS reports

- BROAD OAK: GCHQ's repository of target info
- We match TLS events against this:
  - Is the server IP in BROAD OAK?
  - Does the certificate's domain match a URL selector, or a number of email selectors?
- Email the relevant POC to ask if the traffic is of interest
- About 15% of the services we've identified in this way have been worth looking into further

# FLYING PIG

- TLS knowledge base. Summarises all TLS events to answer multiple questions, e.g.:
  - What certificates are present on a given IP?
  - Which client IPs access a given service?
  - Which TDIs can be associated with a given service?



# Example: search by domain



Prototype owner: [REDACTED]

HRA Justification | Query **FLYING PIG** - general SSL toolkit | Query **QUICK ANT** - Tor events QFD

**Query FLYING PIG**

IP / network / certificate field

Server certificate fields to search within:

Query as:  Client IP  Server IP  Both

or:  Network [e.g. 1.2.3.0/24]

or:  Server Certificate [e.g. %example.com (use % for wildcards)]

Run Query!

Subject common name   
 Subject organisation name   
 Issuer common name   
 Issuer organisation name   
 RSA modulus

Certificate field search:

All HTTP requests matching your query ( ? )

1 - 5 of 500 items | 10 | 25 | 50 | 100

Server IP	Host name	First seen	Last seen	Count w/e 25th Nov	Count all time
.184.105	swa.mail.ru	2011-10-13 16:05:53.0	2011-11-25 21:11:59.0	6085663	42640739
.184.104	swa.mail.ru	2011-10-13 17:29:18.0	2011-11-25 21:11:55.0	6073183	36825411
.134.201	fc.ed.f4.cf.bd.a1.top.mail.ru	2011-10-13 21:43:10.0	2011-11-25 21:10:49.0	4049743	19360920
.135.13	top5.mail.ru	2011-10-14 20:00:00.0	2011-11-25 21:12:05.0	3006868	14168963
.135.12	top3.mail.ru	2011-10-14 20:00:00.0	2011-11-25 21:10:48.0	2480950	12386999

All certificates matching your query ( ? )

Tip 1: Right click on a row to find all server IPs that serve that certificate!  
 Tip 2: Click on the disk icon in the title bar to download data in CSV format!  
 Tip 3: Double-click on a field to enable copy and paste!  
 Tip 4: Change displayed columns ('Basic' is default; 'Advanced' adds RSA Modulus and cipher suite distribution columns):

1 - 10 of 70 items | 10 | 25 | 50 | 100

Full Certificate	First seen	Last seen	Count w/e 25th Nov	Count all time	Valid from	Valid to	Subject common name	Subject country	Subject org name	Issuer common name	Issuer country	Issuer org name	Self signed
308203CD3082(2011-09-22 13:17:32)	2011-11-25 19:01:59	2952729	16638958	2011-01-31 00:00:00	2012-03-27 23:59:59	*.mail.ru	ru	llc mail.ru	thawte ssl ca	us	thawte, inc.	N	
308203613082(2011-09-22 14:05:50)	2011-11-25 18:58:32	249926	1085232	2010-01-21 00:00:00	2011-02-20 23:59:59	*.mail.ru	ru	llc mail.ru	thawte premium server ca	za	thawte consulting cc	N	
308203D33082(2011-10-07 20:29:55)	2011-11-25 18:53:40	10059	30520	2011-09-25 00:00:00	2013-11-23 23:59:59	*.money.mail.ru	ru	llc mail.ru	thawte ssl ca	us	thawte, inc.	N	
308203513082(2011-09-23 17:01:58)	2011-11-25 15:40:05	976	8517	2010-01-25 15:42:05	2012-01-27 18:12:59	mail.ru.is	is	mail.ru.is		us	equifax	N	
308202C83082(2011-08-22 08:14:21)	2011-09-06 06:15:36	0	1482	2011-03-04 06:42:12	2012-03-03 06:42:12	mail.ru-sib.ru	us		mail.ru-sib.ru	us		Y	
308204383082(2011-10-17 14:09:52)	2011-11-25 18:50:10	22	1236	2011-05-27 00:00:00	2012-07-25 23:59:59	mail.ru-com.ru		mail.ru-com.ru	thawte dv ssl ca	us	thawte, inc.	N	
308203C43082(2011-10-08 00:05:24)	2011-11-25 17:04:02	301	1150	2010-02-13 14:19:06	2012-11-08 14:19:06	mx1.shogo-mail.ru	ru	shogo	shogo.ru	ru	shogo	N	
308204153082(2011-11-01 07:36:53)	2011-11-25 14:26:29	246	693	2011-09-15 11:47:51	2012-09-14 11:47:51	limg.s.mail.ru	ru		isp.cegedim.fr	fr	cegedim	N	
308202E43082(2011-10-14 18:20:34)	2011-11-21 05:13:34	201	306	2011-10-05 08:07:34	2014-10-04 08:07:34	moder.foto.mail.ru	ru	mail.ru	moder.foto.mail.ru	ru	mail.ru	Y	
308204153082(2011-10-31 14:14:12)	2011-11-25 15:45:50	99	259	2011-09-15 11:47:51	2012-09-14 11:47:51	auth.mail.ru	ru		isp.cegedim.fr	fr	cegedim	N	

Server IPs ( ? )

Tip 1: Right click on a server IP to explore it further!

1 - 25 of 500 items | 1 | 2 | 3 | 4 | 5 | 6 | 7

Server IP	Cert count w/e 25th Nov	Cert count all time
.184.104	257542	2250170
.177.1	333592	1052618
.191.213	330212	1388617
.184.16	308599	2496916
.184.17	297282	2226133
.184.15	294437	2395012
.189.160	168414	659037
.184.77	120533	560336
.184.74	113555	515169
.184.75	112574	538512
.184.76	110325	690098
.135.55	3779	6023
.135.56	3740	7358
.134.151	3564	8498
.63.121	2532	4887
.136.43	2523	9226
.134.98	2360	9165
.179.89	2227	7600
.179.90	2051	7320
.136.84	1981	8442

Explore this server IP further!

# Example: search by server IP

ID



Prototype owner: [REDACTED]

HRA Justification Query FLYING PIG - general SSL toolkit Query QUICK ANT - Tor events QFD

**Query FLYING PIG**  
 IP / network / certificate field   
 Query as:  Client IP  Server IP  Both  
 or:  Network [e.g. 1.2.3.0/24]  
 or:  Server Certificate [e.g. %example.com (use % for wildcards)]

**General IP info**  
 Top 10 SSL client geos  
 Top 10 SSL server ports  
 Top 10 SSL case notations  
 SSL Traffic stats

**Server IP-specific panels**  
 SSL Server certificates seen on this IP  
 SSL Pattern of life  
 HTTP requests to this IP  
 Top 100 SSL clients

Certificate field search: %mail.ru Server IP: 184.14

**General IP info for server IP 184.14**

<b>Geolocation ( ? ):</b> Country: RU (M) City: MOSCOW (L)	<b>WHOIS info ( ? ):</b> Network: 184.14.0.0/20. Network type: No results. Company: Mail.Ru. Domain: mail.ru.	<b>AS info ( ? ):</b> Advertised by AS: 47764. Found within network: 76.0/20. AS name: MAILRU-AS Limited liability company Mail.Ru.	<b>DNS ( ? ):</b> No results	<b>Tor node ( ? ):</b> No matches
--	---	---	---------------------------------	--------------------------------------

<b>Top 10 SSL client geos ( ? )</b> 	<b>Top 10 SSL server ports ( ? )</b> 	<b>Top 10 SSL case notations ( ? )</b> Overall Paired (approximate)	<b>SSL Traffic stats ( ? ):</b> For week ending 2011-12-23: No. unique clients = 104317. % client-server IPs with traffic seen in both directions = 14.7%.  Legend: Unique clients with client-server traffic only, Unique clients with server-client traffic only, Unique clients with bidirectional traffic
---	--	---	--

**SSL Certificates seen on this IP ( ? )**  
 Tip 1: Right click on a certificate to explore it further!

1 - 3 of 3 items | 10 | 25 | 50 | 100

First seen on this IP	Last seen on this IP	Count w/e 25th Nov	Count all time	Valid from	Valid to	Subject common name	Issuer common name
2011-09-22 13:31:06	2011-11-25 19:01:47	357643	2359179	2011-01-31 00:00:00	2012-03-27 23:59:59	*.mail.ru	thawte ssl ca
2011-08-08 12:23:45	2011-11-25 07:50:07	1441	1447304	2011-01-31 00:00:00	2012-03-27 23:59:59	*.mail.ru	thawte ssl ca
2011-11-16 14:13:03	2011-11-16 14:13:03	0	1	2011-08-05 18:34:19	2014-08-05 18:34:19	*.vkontakte.ru	go daddy secure certification authority

**Average pattern of life for a client (seeded around SSL events to this server IP) ( ? )**  
 Tip 1: Filter by min. % occurrences of event: 1% Apply filtering

1 - 8 of 233 items | 10 | 25 | 50 | 100

Correlated event	Event IP	Event port	Percentage occurrences of event
GET request to top3.mail.ru	.135.12	80	28.1
GET request to top5.mail.ru	.135.13	80	15.1
GET request to d0.c1.bf.a1.top.mail.ru	.134.253	80	14.2
GET request to mx.mail.ru	.184.40	80	13.2

**HTTP requests to this IP (top 100) ( ? )**  
 Tip 1: Right click on a server IP to explore it as an SSL server!

1 - 10 of 226 items | 10 | 25 | 50 | 100

Server IP	Host name requested	First seen	Last seen	Count last week	Count all time
.184.14	e.mail.ru	2011-10-14	2011-11-25	1989215	13992636
.184.14	m.mail.ru	2011-10-14	2011-11-25	89268	664189
.184.14	.184.14	2011-10-14	2011-11-25	17426	108536
.184.14	auth.mail.ru	2011-10-14	2011-11-25	11738	70020
.184.14	tel.mail.ru	2011-10-14	2011-11-25	8084	65540

# Contacts

- TLS trends: Crypt Operations  
BULLRUN team
  - [REDACTED]@gchq)
  - [REDACTED]@gchq)
- FLYING PIG: ICTR Network  
Exploitation
  - [REDACTED]@gchq)