Decrease Your Circle of Trust: An Investigation of PKI CAs on Mobile Devices

Andrew Blaich, PhD

Lead Security Analyst
Bluebox Security
@ablaich
Who are you trusting?

- How much trust do you put in your phone?
  - How many vendors have modified your OS?
  - How many applications and services are running on your device?
  - How many libraries are loaded for an app?
  - How many roots of trust exist for network connections?
Who are you trusting?

- How much trust do you put in your phone?
  - How many vendors have modified your OS?
    - Google -> Samsung -> Qualcomm -> AT&T -> Others?
  - How many applications and services are running on your device?
    - 300+ apps/services on a Samsung Galaxy Note 3
  - How many libraries are loaded for an app?
    - 100+ shared libraries on a Samsung Galaxy Note 3
  - How many entities are trusted for network connections?
    - 150 + on Android
    - 200+ on iOS
Circle of Trust

- OEMs
- Libs
- Apps
- CAs
- Component Suppliers
- Carriers

Trust

Circle
Trustable by Bluebox

Example of a brand new out of the box device and all the entities that you would trust on it.
Same device, different carriers
### Vulnerability analysis

- **Android Masterkey(s): protected**
- **Android FakelID: protected**
- **Heartbleed (OS only): protected**
- **Linux futex (Towelroot): protected**
- **ObjectInputStream Serialization: protected**
- **Settings PendingIntent (BroadAnywhere): vulnerable**
- **GraphicsBuffer Overflow: vulnerable**

[View vulnerability info](#)

### Your device trusts...

- **345 total installed apps/packages**
- **156 roots of trust/certificate authorities**
- **70 apps with dangerous-level permissions**
- **69 apps with system-level privileges**
- **49 apps that can send your data to the Internet**
- **39 third-party apps included with your device**
- **18 apps to read all your personal contacts**
- **12 apps with extra privileges**
- **12 apps to read your SMS messages**
- **8 apps that can install other apps**
- **7 apps to make phone calls**
- **4 apps that can control cellular data**
- **1 active device administration apps**

[View further details](#)

---

**Mobile security awareness by Bluebox**

Contact sales@bluebox.com for corporate & MDM-enabled version of this application

---

**Mobile security awareness by BLUE BOX**

Contact sales@bluebox.com for corporate & MDM-enabled version of this application

---

**Mobile security awareness by BLUE BOX**

Contact sales@bluebox.com for corporate & MDM-enabled version of this application
Circle of Trust

- OEMs
- Libs
- Apps
- CAs
- Component Suppliers
- Carriers

Trust

Circle
Circle of Trust
Secure Connections

Apps | CAs | Network
The Hellenic Academic and Research Institutions Certification Authority (HARICA) is a non-profit activity operated by the Greek Universities Network (www.gunet.gr). Our main website is www.harica.gr and has been operating since 2006. All of our certificates have a clear mark indicating that "This certificate is subject to Greek laws and our CPS. This Certificate must only be used for academic, research or educational purposes". This is also included in the comments and policy fields of each certificate.

The main goal of HARICA is the deployment of an infrastructure for secure communication between the administrative systems of the Greek Academic and Research Institutions.

only be used for academic, research or educational purposes".
iOS 8: List of available trusted root certificates

The iOS Trust Store contains trusted root certificates that are preinstalled with iOS.

About trust and certificates

The iOS Trust Store is the place where iOS stores signed apps and their certificates. The Trust Store stores all of the certificates in an immutable format, so you can't alter trusted certificates, and is used by the operating system to determine whether a certificate is valid and whether an app that's using the certificate is safe to install and run.

```
Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: shalWithRSAEncryption
Issuer: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions RootCA 2011
Trust: Always
Validity
  Not Before: Dec 6 13:49:52 2011 GMT
  Not After: Dec 1 13:49:52 2031 GMT
Subject: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions RootCA 2011
Subject Public Key Info:
```

...
Google Chrome will banish Chinese certificate authority for breach of trust [Updated]
Draconian move follows the issuance of certificates masquerading as Google domains.

by Dan Goodin - Apr 1, 2015 8:55pm PDT
Google Chrome will banish Chinese certificate authority for breach of trust
[Updated]
Draconian move follows the issuance of certificates masquerading as

by Dan Goodin - Apr 1, 2015 8:55pm PDT
Not only browsers…
Certificate Authorities

- What certificate authorities are on my device?
- How many are there?
- Who are these certificate authorities?
- How did they get on my device?
- What security concerns are there?
Objectives

- Learn more about who your device is trusting
- Learn about the roles CAs play in secure communications
- Learn the history behind these CAs
- Learn how you can take action to decrease your circle of trust
Background - Certificate Authorities
Body

- What is a CA?
- How do they get on the device?
- How many are there?
- User installable vs. system pre-loaded (also talk about carrier and OEM additions or removals)
- iOS VPN and Android VPN case study
Certificate Authorities

 What is a certificate authority?
 They validate that who you are talking to is who they say they are

Trusted CAs: CA-A

Are you Google.com?

Yes, CA-A says I am.

TRUSTED CONNECTION
Certificate Authorities

- What is a certificate authority?
  - They validate that who you are talking to is who they say they are

Trusted CAs: CA-A

Google

Are you Google.com?

Yes, CA-M says I am.

NOT TRUSTED CONNECTION
CA Chain of Trust

- What is the chain of trust?
Trusted Certificate Chain

The root CA to verify this chain is installed on the device making the trust chain verifiable and thus it is considered a trusted and secured connection.
Un-trusted Certificate Chain

Un-verified == Un-Trusted Chain

The root CA to verify this chain is missing from this device making the trust chain un-verifiable and thus not-trusted and in-secure.
Types of Root CAs

- Pre-installed root CAs
- User-installed root CAs
Why is this a concern?

- A malicious or compromised root CA can read your secure traffic
- CNNIC and MCS Holdings
- Lenovo and Superfish
- …
Pre-installed Root CAs
Root CA Approval Process

Root Certificate Programs

- Mozilla
- Microsoft
- Apple
- others
### Mozilla Root CA Approval Process

#### How a CA gets included into Firefox
[Timeline](https://wiki.mozilla.org/CA:How_to_apply#Timeline)

- **Information Verification**: ~2 months
- **First Public Discussion**: ~2 months
- **Second Public Discussion**: ~4 weeks
- **Inclusion in NSS**: ~1 week, ~3 months
- **Inclusion in Firefox**: ~2 months
- **Finished**

The whole process can take approximately 11 months or more.

Linux and Android are strongly tied to the Mozilla process.
CA Trust Infrastructure

- The effectiveness of the global PKI trust infrastructure relies on keeping the designated roots of trust fully secure and operating correctly.

**Trusted Root CAs**

- CA -A
  - Issue cert for *.google.com
  - No.

- CA -B
  - Issue cert for *.google.com
  - Ok.

- Compromised CA
CAs on Mobile Devices

5.1
8.3

162 System Installed Certificates
227
Root CA Reference Links

- **iOS:**
  - Trusted
  - Always Ask
  - Blocked

- **Android:**
CA Classifications

- Known Failures in Keeping Trust
- Government-Based Roots of Trust
- Cause for Concern
- Artificial Constraints
- Everything else
Known Failures
Known Failures with CAs

- “Hacked” CAs:
  - CNNIC/MCS Holdings [2015]
  - Comodo [2011]
  - DigiNotar [2011]
  - GlobalSign [2011]
  - India CCA [2014]
  - RapidSSL (indirect) [2008]
# Apple’s Blocked CA List

<table>
<thead>
<tr>
<th>CA Name</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>TurkTrust</td>
<td>Issued an inappropriate sub-CA cert that was used to issue a *.google.com cert</td>
</tr>
<tr>
<td>Entrust</td>
<td>Issued a wildcard cert for Apple domains</td>
</tr>
<tr>
<td>GTE CyberTrust Solutions</td>
<td>Issued 4 sub-CA certs for DigiNotar</td>
</tr>
<tr>
<td>DigiNotar</td>
<td>Issued itself another sub-CA cert</td>
</tr>
<tr>
<td>Entrust</td>
<td>Issued 2 sub-CA certs for DigiNotar</td>
</tr>
<tr>
<td>Entrust</td>
<td>Issued a sub-CA cert for Digicert Sdb. Bhd (practices of this CA in Malaysia were found to be inappropriate)</td>
</tr>
</tbody>
</table>
Apple’s Blocked CA List – cont’d.

<table>
<thead>
<tr>
<th>CA Name</th>
<th>Reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>GTE</td>
<td>Issued a sub-CA cert for Digicert Sdb. Bhd</td>
</tr>
<tr>
<td>Trustwave</td>
<td>Issued a sub-CA cert to Micros Systems</td>
</tr>
<tr>
<td>Xramp</td>
<td>Issued a sub-CA cert to Trustwave</td>
</tr>
<tr>
<td>TurkTrust</td>
<td>Issued a sub-CA cert to KKTC Merkez Bankasi</td>
</tr>
</tbody>
</table>
Government CAs
Government Related CAs

Government CAs
- Govt. of Spain
- ACCV
- Govt. of Hong Kong
- Post Root
- Govt. of Netherlands
- Staat der Niederlanden
- Govt. of South Korea
- KISA
- Govt. of Japan
- Spanish FNMT

Suspected of affiliation with a government entity
- JCSI
- SecureSign
- Agencia Catalana de Certificacio
- SOCIEDAD CAMERAL DE CERTIFICACION
- Chunghwa Telecom Co

Other nationally-operating entities
- AC Camerfirma S.A.
- Autoridad de Certificado
  n Firmaprofesional
- TURKTRUST
- CNNIC
- e-tugra
- HARICA
- Elektronik Biili Guvenligi
  A.S.

Allowed to use an internal audit for approval.
Causes for Concern - CAs
Causes for Concern

Issued improper certificates
- SecureTrust Corporation
  - Secure Global CA
  - SecureTrust CA
- Government of France (PM/SGDN)
  - DCSSI

Deprecated
- Certicámara S.A.
  - AC Raíz Certicámara S.A.
- TDC Internet
  - TDC Internet Root CA

TÜRKTRUST
  - TÜRKTRUS T .... (c) Aralık 2007
Causes for Concern – cont’d.

Community Controversy

- Staat der Nederlan
den
  - Staat der Nederl
den Root CA
  - Staat der Nederl
den Root CA -
    G2
  - HARICA
    - Hellenic Academ
cic and Research
    Institutions RootCA 2011

- StartCom Ltd.
  - StartCom Certification
    Authority
  - StartCom Certification
    Authority G2
  - CNNIC
    - CNNIC ROOT
Causes for Concern – cont’d.
Artificial Constraints
# Artificial Constraints

<table>
<thead>
<tr>
<th>Cert Subject</th>
<th>Reason For Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN=IGC/A,OU=DCSSI,O=PM/SGDN,L=Paris,ST=France,C=FR</td>
<td>Issued several un-authorized certificates for Google domains. TLD restrictions: .fr (France), .gp (Guadeloupe), .gf (Guyane), .mq (Martinique), .re (Réunion), .yt (Mayotte), .pm (Saint-Pierre et Miquelon), .bl (Saint Barthélemy), .mf (Saint Martin), .wf (Wallis et Futuna), .pf (Polynésie française), .nc (Nouvelle Calédonie), .tf (Terres australes et antarctiques françaises)</td>
</tr>
</tbody>
</table>
Artificial Constraints –cont’d.

// static
bool CertVerifyProc::HasNameConstraintsViolation()
{
    const HashValueVector& public_key_hashvec =
        const std::string& common_name,
    const std::vector<std::string>& dns_names,
    const std::vector<std::string>& ip_addrs) {
    static const char kDomainsANSSI[][kMaxDomainLength] = {
        "fr", // France
        "gp", // Guadeloupe
        "gf", // Guyane
        "mq", // Martinique
        "re", // Réunion
        "yt", // Mayotte
        "pm", // Saint-Pierre et Miquelon
        "bl", // Saint Barthélemy
        "mf", // Saint Martin
        "wf", // Wallis et Futuna
        "pf", // Polynésie française
        "ac", // Nouvelle-Calédonie
        "tf", // Territoires australiens et antarctiques françaises
    };
    static const char kDomainsIndiaCCA[][kMaxDomainLength] = {
        "gov.in",
        "nic.in",
        "ac.in",
        "rbi.org.in",
        "bankofindia.co.in",
        "ncoode.in",
        "tes.co.in",
    };
}
Artificial Constraints – cont’d.
## Apple’s Extended Trust

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Federal Certificates</td>
<td>5</td>
<td>4 are not on Android</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 is under review by Mozilla</td>
</tr>
<tr>
<td>Present on iOS, but requested for removal on Mozilla/Android</td>
<td>3</td>
<td>2 deprecated from AOL/Time Warner</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 deprecated from Danish IT</td>
</tr>
<tr>
<td>Other Entities added by Apple</td>
<td>15</td>
<td>5 from Apple</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 from Denmark</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 from Swiss Government</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 from Belgium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 from Cisco</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 from Czech Republic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 from Canada</td>
</tr>
</tbody>
</table>
CA Cryptography Analysis
# Public Key-Size

<table>
<thead>
<tr>
<th>Key Type/Size</th>
<th>Count</th>
<th>Notable Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elliptic Curve</td>
<td>6</td>
<td>GeoTrust, VeriSign, COMODO, Thawte, Entrust, AffirmTrust</td>
</tr>
<tr>
<td>RSA / 1024 bit</td>
<td>15</td>
<td>FNMT, GTE CyberTrust, Equifax, Netlock, Halozatbiztonsagi, VeriSign, ValiCert, Thawte Consulting, Entrust</td>
</tr>
<tr>
<td>RSA / 2048 bit</td>
<td>101</td>
<td>N/A</td>
</tr>
<tr>
<td>RSA / 4096 bit</td>
<td>14</td>
<td>N/A</td>
</tr>
</tbody>
</table>
# Hash Algorithm

<table>
<thead>
<tr>
<th>Signature Algorithm</th>
<th>Count</th>
<th>Notable Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>ecdsa-with-SHA384</td>
<td>6</td>
<td>GeoTrust, VeriSign, COMODO, Thawte, Entrust, AffirmTrust</td>
</tr>
<tr>
<td>md5WithRSAEncryption</td>
<td>6</td>
<td>GTE, Netlock, Equifax</td>
</tr>
<tr>
<td>sha1WithRSAEncryption</td>
<td>115</td>
<td>N/A</td>
</tr>
<tr>
<td>sha256WithRSAEncryption</td>
<td>28</td>
<td>N/A</td>
</tr>
<tr>
<td>sha384WithRSAEncryption</td>
<td>1</td>
<td>N/A</td>
</tr>
</tbody>
</table>
CA Consolidation

<table>
<thead>
<tr>
<th>Symantec Owned Entity</th>
<th>Number of Certificates on Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>GeoTrust</td>
<td>7</td>
</tr>
<tr>
<td>Verisign</td>
<td>7</td>
</tr>
<tr>
<td>TC Trust Center</td>
<td>3</td>
</tr>
<tr>
<td>Network Solutions</td>
<td>1</td>
</tr>
<tr>
<td>Thawte</td>
<td>5</td>
</tr>
<tr>
<td>Equifax</td>
<td>3</td>
</tr>
<tr>
<td><strong>Total:</strong> 156 certificates</td>
<td>Symantec controls 25 of the total 156 certificates or ~16% ownership of the Android roots of trust</td>
</tr>
</tbody>
</table>
CA Consolidation – cont’d.
CA Consolidation – cont’d.

- GTE
  - subsidiary
  - resulted in Verizon Business
  - sold to CyberTrust
    - subsidiary of GTE
      - merger
      - resulted in BeTrusted
        - merger
        - resulted in TruSecure
  - bought by Verizon Business
  - bought by TruSecure
  - bought by Ubizen
Some OEMs and carriers add additional certificates into the ROM that are not found in AOSP:

- Sony Xperia running 4.4.4 includes two root certs for Sony
- iOS has several additional certificates that Android does not currently* have e.g.: Cisco and US Government
User-installed Root CAs
User installed root CAs

Network monitoring

A third party is capable of monitoring your network activity, including emails, apps, and secure websites.

A trusted credential installed on your device is making this possible.

Check trusted credentials
VPN Case-Study
VPN, Anonymization, Privacy Providers

- Looked at 10 of the top VPN Service Provider services in the Apple App Store and the Google Play Store:
  - iOS – App Store
    - 6 out of 10 of the iOS Apps used an MDM VPN Profile that DID install a 3rd party certificate
  - Android – Google Play Store
    - 10 out of 10 of the Play Store apps did not install a 3rd party certificate
Decreasing your Trust Circle

- **Android:**
  - Manually
  - Settings -> Security -> Trusted credentials
  - Disable or Enable each CA

- **iOS:**
  - No direct method on iOS…
Bluebox Trust Managers

https://bluebox.com/technical/trust-managers/
Summary

- Learn more about who your device is trusting
  - iOS and Android have an increasing amount of roots of trust
- Learn about the roles CAs play in secure communications
  - Without a CA we cannot verify that who we are talking to is legitimate
- Learn the history behind these CAs
  - Sometimes things go wrong with CAs
- Learn how you can take action to decrease your circle of trust
  - Manual certificate management
  - Bluebox Trust Manager for iOS and Android
Apply

- Learn more about what your device is trusting:
  - Trustable by Bluebox
- View the root CAs on your device:
  - Android System Settings
  - Bluebox Trust Manager (Android and iOS)
- Manage the root CAs on your device (root/jailbreak) required:
  - Android System Settings
  - Bluebox Trust Manager (Android and iOS)