Flipped Classroom Session 8: PKI and TLS

CS-E3130 Information Security, 5.10.2023

1. X.509 Certificates

1.1. Critical extensions

Some extensions in a certificate contain a "critical" tag, which indicates that software using the certificate must raise an error if it doesn't understand the extension.

Which kinds of extension make sense to mark as critical, and which do not? Give an example of each.

1.2. Trusting the contents of a certificate

An X.509 certificate contains both the identity of the subject (the entity that the certificate "is about"), and the issuer (the entity that produced the certificate)). For example,

```
Issuer: C = US, O = Amazon, CN = Amazon RSA 2048 M02
Subject: CN = gunn.ee
```

If we trust the issuer named in the certificate, does this mean that we can trust that the public key in the certificate really belongs to the subject? Why (not)?

2. Public Key Infrastructure in the browser

2.1. Certificate chain validation

Consider the following certificates, obtained by running

```
openssl s_client -showcerts gunn.ee:443
```

and then copying the certificates from the output and processing them with

```
openssl x509 -in <cert>.pem -text -fingerprint
```

to obtain the output below. Explain in detail how a web browser checks this specific certificate chain, and how the browser uses it to authenticate the website in TLS.

Notes:

- You do not need to explain the details of the TLS handshake protocol, or Certificate Transparency
- The fingerprint at the bottom of each certificate is computed by OpenSSL, and can be trusted to be a correct hash of the rest of the certificate
- You can refer to Mozilla's database of trusted Certificate Authorities at https://ccadb.my.salesforce-sites.com/mozilla/IncludedCACertificateReport.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            08:a9:d1:a3:b7:69:bc:5f:4e:21:b2:75:c5:44:91:14
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Amazon, CN = Amazon RSA 2048 M02
        Validity
            Not Before: Aug 28 00:00:00 2023 GMT
            Not After : Sep 24 23:59:59 2024 GMT
        Subject: CN = gunn.ee
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a8:6a:ee:f5:fb:1c:bf:8b:18:bb:1c:b8:ac:db:
                    cc:46:6d:3d:75:e1:cf:5e:9c:03:24:d2:be:21:64:
                    e5:0d:f4:dd:a1:85:47:48:1f:df:b1:bb:e2:a6:5a:
```

```
                    d7:1e:f7:fa:e1:78:0a:7b:f0:37:0e:c9:03:77:ad:
                    29:6d:91:b3:4d:8c:0e:d6:b2:4d:5d:b2:d5:aa:b8:
                    b6:c2:80:c4:44:a9:fe:fa:44:ef:9d:0c:f7:26:7e:
                    14:dc:1b:e1:07:35:26:e8:e0:e6:db:a0:5d:cb:f6:
                    6a:8e:28:69:ae:22:31:0f:61:cd:cb:b5:21:c9:85:
                    97:ac:d7:3e:37:85:f0:b3:73:a8:49:1f:7a:db:5f:
                    f8:0d:aa:d0:c3:89:af:a1:a7:b0:9a:56:f8:98:bc:
                    a1:fc:90:50:69:e9:10:ca:76:e2:49:bd:6e:81:ab:
                    0a:da:95:4b:33:79:7e:3b:be:de:c8:f9:70:07:24:
                    2e:03:e7:6c:24:ca:d4:22:14:e8:19:97:b4:d9:6d:
                    c8:46:dc:7d:7d:e3:67:38:24:2e:57:c3:39:ff:83:
                    6b:b2:e9:88:bb:80:b3:c4:5e:67:e9:22:33:55:13:
                    01:76:f5:af:42:03:8f:ac:53:28:83:0a:67:e7:55:
                    f9:94:48:71:22:7d:ca:1f:1c:7b:de:80:05:44:2c:
                    b4:d3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                C0:31:52:CD:5A:50:C3:82:7C:74:71:CE:CB:E9:9C:F9:7A:EB:82:E2
            X509v3 Subject Key Identifier:
                0B:20:05:54:10:14:B2:7D:30:7F:86:12:27:E7:17:CB:71:63:E3:83
            X509v3 Subject Alternative Name:
                DNS:gunn.ee, DNS:lachlan.gunn.ee, DNS:www.gunn.ee, DNS:www.lachlan.gunn.ee
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.r2m02.amazontrust.com/r2m02.crl
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
            Authority Information Access:
                OCSP - URI:http://ocsp.r2m02.amazontrust.com
                CA Issuers - URI:http://crt.r2m02.amazontrust.com/r2m02.cer
            X509v3 Basic Constraints: critical
                CA:FALSE
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : EE:CD:D0:64:D5:DB:1A:CE:C5:5C:B7:9D:B4:CD:13:A2:
                                32:87:46:7C:BC:EC:DE:C3:51:48:59:46:71:1F:B5:9B
                    Timestamp : Aug 28 10:18:54.434 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:46:02:21:00:D9:C7:11:6C:0E:19:F6:48:9B:76:70:
                                02:B9:1E:5A:03:98:16:9E:84:EB:53:9B:2C:04:7B:35:
                                1F:A6:5A:CF:B6:02:21:00:CB:BD:32:75:99:36:38:ED:
                                8A:15:61:7E:48:8F:41:40:91:0E:78:E6:EA:37:3C:2D:
                                2C:59:22:1F:0A:E2:15:DD
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB:
                                1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73
                    Timestamp : Aug 28 10:18:53.987 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:46:02:21:00:9C:2F:B0:E9:03:51:4E:DE:CF:00:61:
                                6E:23:E3:67:78:28:55:CE:30:6F:20:EC:9E:0E:59:48:
                                9E:4C:D6:C6:14:02:21:00:A9:29:45:D0:16:9B:00:2F:
                                84:CD:98:8F:AA:5A:E6:94:C9:36:BA:8A:79:28:D3:9A:
                                9F:38:24:6C:7E:41:5E:3E
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : DA:B6:BF:6B:3F:B5:B6:22:9F:9B:C2:BB:5C:6B:E8:70:
                                91:71:6C:BB:51:84:85:34:BD:A4:3D:30:48:D7:FB:AB
                    Timestamp : Aug 28 10:18:53.898 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:46:02:21:00:8F:4C:27:0F:38:CF:28:47:40:25:1D:
                                30:6A:10:5B:39:27:89:98:5C:F9:B9:A2:F2:97:7A:EC:
                                0E:02:99:66:7C:02:21:00:B1:1D:C4:8F:75:29:13:2E:
                                5F:38:75:1D:39:35:B8:1B:5B:97:C3:A6:6C:46:96:BF:
                                78:88:04:92:1F:20:AC:4B
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        29:89:bd:0a:42:8a:92:61:ca:76:bd:7c:82:38:21:7f:7c:d2:
        86:17:e4:b1:db:62:4d:1a:63:c6:a7:17:59:8d:32:de:d5:0a:
        00:65:ca:85:8e:98:74:0d:a5:28:b0:8a:32:e9:73:fb:08:f5:
        c5:a9:d9:7f:5e:f6:57:9f:9c:ba:e8:1b:52:13:9e:53:f7:d1:
        50:c9:fb:43:f1:80:dc:e1:64:2f:69:6a:4b:ea:1b:f6:a8:e2:
        d5:16:be:98:fb:46:ac:ec:72:3a:90:f3:9a:88:18:11:48:6f:
        29:1c:1d:10:08:d4:8e:63:06:97:79:4b:6d:75:1d:b6:30:94:
        67:4a:cc:d7:4f:c5:a0:f4:fb:6b:fe:cf:5f:13:7b:86:ba:cd:
        08:0e:eb:0f:f1:76:34:8f:7b:1a:56:78:d0:ff:e5:69:52:38:
        40:2d:b9:1d:31:89:ce:45:2f:84:cf:e6:91:c3:63:d6:4e:cf:
        72:cf:41:cb:35:ff:b8:56:55:91:ca:e7:bd:46:fd:06:19:8e:
        03:0b:34:32:96:05:bf:60:d0:db:45:24:63:34:dd:8e:5a:0a:
        91:f2:26:14:d0:1d:ff:f0:c9:c0:36:3e:9b:c1:2e:30:29:7a:
        d9:11:9d:39:fc:93:bb:6c:56:4d:1d:eb:73:f1:57:e3:a7:ac:
        fa:d6:79:a5
SHA1 Fingerprint=8F:88:CB:7B:E2:CC:01:08:45:FE:23:30:2E:50:17:54:E1:BF:B7:3F
-----BEGIN CERTIFICATE-----
MIIF8DCCBNigAwIBAgIQCKnRo7dpvF9OIbJ1xUSRFDANBgkqhkiG9w0BAQsFADA8
MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRwwGgYDVQQDExNBbWF6b24g
UlNBIDIwNDggTTAyMB4XDTIzMDgyODAwMDAwMFoXDTI0MDkyNDIzNTk1OVowEjEQ
MA4GA1UEAxMHZ3Vubi5lZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AKhq7vX7HL+LGLscuKzbzEZtPXXhz16cAyTSviFk5Q303aGFR0gf37G74qZa1x73
+uF4CnvwNw7JA3etKW2Rs02MDtayTV2y1aq4tsKAxESp/vpE750M9yZ+FNwb4Qc1
Jujg5tugXcv2ao4oaa4iMQ9hzcu1IcmFl6zXPjeF8LNzqEkfettf+A2q0MOJr6Gn
```

```
sJpW+Ji8ofyQUGnpEMp24km9boGrCtqVSzN5fju+3sj5cAckLgPnbCTK1CIU6BmX
tNltyEbcfX3jZzgkLlfDOf+Da7LpiLuAs8ReZ+kiM1UTAXb1r0IDj6xTKIMKZ+dV
+ZRIcSJ9yh8ce96ABUQstNMCAwEAAaOCAxYwggMSMB8GA1UdIwQYMBaAFMAxUs1a
UMOCfHRxzsvpnPl664LiMB0GA1UdDgQWBBQLIAVUEBSyfTB/hhIn5xfLcWPjgzBF
BgNVHREEPjA8ggdndW5uLmVlgg9sYWNobGFuLmd1bm4uZWWCC3d3dy5ndW5uLmVl
ghN3d3cubGFjaGxhbi5ndW5uLmVlMA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAU
BggrBgEFBQcDAQYIKwYBBQUHAwIwOwYDVR0fBDQwMjAwoC6gLIYqaHR0cDovL2Ny
bC5yMm0wMi5hbWF6b250cnVzdC5jb20vcjJtMDIuY3JsMBMGA1UdIAQMMAowCAYG
Z4EMAQIBMHUGCCsGAQUFBwEBBGkwZzAtBggrBgEFBQcwAYYhaHR0cDovL29jc3Au
cjJtMDIuYW1hem9udHJ1c3QuY29tMDYGCCsGAQUFBzAChipodHRwOi8vY3J0LnIy
bTAyLmFtYXpvbnRydXN0LmNvbS9yMm0wMi5jZXIwDAYDVR0TAQH/BAIwADCCAYEG
CisGAQQB1nkCBAIEggFxBIIBbQFrAHcA7s3QZNXbGs7FXLedtM0TojKHRny87N7D
UUhZRnEftZsAAAGKO6dMYgAABAMASDBGAiEA2ccRbA4Z9kibdnACuR5aA5gWnoTr
U5ssBHs1H6Zaz7YCIQDLvTJ1mTY47YoVYX5Ij0FAkQ545uo3PC0sWSIfCuIV3QB3
AEiw42vapkc0D+VqAvqdMOscUgHLVt0sgdm7v6s52IRzAAABijunSqMAAAQDAEgw
RgIhAJwvsOkDUU7ezwBhbiPjZ3goVc4wbyDsng5ZSJ5M1sYUAiEAqSlF0BabAC+E
zZiPqlrmlMk2uop5KNOanzgkbH5BXj4AdwDatr9rP7W2Ip+bwrtca+hwkXFsu1GE
hTS9pD0wSNf7qwAAAYo7p0pKAAAEAwBIMEYCIQCPTCcPOM8oR0AlHTBqEFs5J4mY
XPm5ovKXeuw0AplmfAIhALEdxI91KRMuXzh1HTk1uBtbl8OmbEaWv3iIBJIfIKxL
MA0GCSqGSIb3DQEBCwUAA4IBAQApib0KQoqSYcp2vXyCOCF/fNKGF+Sx22JNGmPG
pxdZjTLe1QoAZcqFjph0DaUosIoy6XP7CPXFqdl/XvZXn5y66BtSE55T99FQyftD
8YDc4WQvaWpL6hv2qOLVFr6Y+0as7HI6kPOaiBgRSG8pHB0QCNSOYwaXeUttdR22
MJRnSszXT8Wg9Ptr/s9fE3uGus0IDusP8XY0j3saVnjQ/+VpUjhALbkdMYnORS+E
z+aRw2PWTs9yz0HLNf+4VlWRyue9Rv0GGY4DCzQylgW/YNDbRSRjNN2OWgqR8iYU
0B3/8MnANj6bwS4wKXrZEZ05/JO7bFZNHetz8Vfjp6z61nml
-----END CERTIFICATE-----
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            07:73:12:4a:4b:cb:d4:4e:c7:b5:3b:ea:f1:94:84:2d:3a:0f:a1
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Amazon, CN = Amazon Root CA 1
        Validity
            Not Before: Aug 23 22:25:30 2022 GMT
            Not After : Aug 23 22:25:30 2030 GMT
        Subject: C = US, O = Amazon, CN = Amazon RSA 2048 M02
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bb:43:18:c6:5a:a8:79:de:29:e8:b5:6f:2e:be:
                    a5:43:cf:2e:58:d3:07:5e:37:4a:2e:95:a4:45:8f:
                    73:a9:92:90:58:59:6f:fe:aa:ae:46:72:a0:79:50:
                    2d:b0:d8:9c:8d:83:ee:10:f4:b1:dc:c4:a9:f9:ee:
                    02:32:2c:b9:74:0b:1b:70:3c:4e:f5:fa:57:7a:05:
                    34:11:55:7b:c3:65:2c:91:ef:06:c7:8a:63:cf:2c:
                    68:bc:2e:7f:19:19:57:09:3b:e2:0e:27:5a:53:4c:
                    5f:39:5a:f5:8e:45:df:0c:11:1f:03:15:1f:8e:37:
                    c4:6c:fa:52:d1:92:65:2a:90:f7:87:85:c7:95:fb:
                    4e:5a:ad:f3:08:62:f2:a0:9a:29:d6:79:ac:d6:a4:
                    fa:bf:67:51:38:4e:78:29:6a:15:de:28:5f:27:21:
                    ff:f4:5c:ed:8d:1e:5f:52:8d:58:76:12:23:53:64:
                    df:59:98:82:22:b7:26:f1:f4:eb:78:3e:2b:db:47:
                    03:ad:d9:79:38:0a:82:77:65:87:e5:88:fb:3b:fb:
                    8b:8e:07:7a:94:59:8c:0d:45:63:06:19:f5:5b:ff:
                    f5:49:02:e5:8c:fc:ff:25:3a:e5:f8:23:68:4f:b0:
                    54:73:38:7b:f6:32:0b:6a:2c:ac:f5:84:ee:02:7e:
                    75:73
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Key Identifier:
                C0:31:52:CD:5A:50:C3:82:7C:74:71:CE:CB:E9:9C:F9:7A:EB:82:E2
            X509v3 Authority Key Identifier:
                84:18:CC:85:34:EC:BC:0C:94:94:2E:08:59:9C:C7:B2:10:4E:0A:08
            Authority Information Access:
                OCSP - URI:http://ocsp.rootca1.amazontrust.com
                CA Issuers - URI:http://crt.rootca1.amazontrust.com/rootca1.cer
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.rootca1.amazontrust.com/rootca1.crl
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        2d:4e:2e:85:b3:40:33:7e:2f:a2:c2:6e:e3:af:3f:82:4b:11:
        c7:fa:e1:e5:ec:b6:b0:dc:c4:12:5d:5b:51:f1:15:79:dc:fb:
        51:ea:bf:fa:80:da:6a:97:37:68:66:ae:05:29:b0:03:8b:5b:
        fd:06:e9:fc:45:8f:03:e7:5b:9e:75:17:e3:b1:b7:a8:76:2c:
        de:04:1f:27:5e:67:b2:0f:7d:c4:a7:b5:40:4e:3e:28:cd:c7:
        77:d5:81:55:7e:04:61:bd:34:b1:36:ba:d3:94:da:56:91:49:
        34:9b:70:4c:3e:ff:2c:83:7f:35:1e:10:3a:b8:46:28:90:4e:
        6a:f6:ec:2c:ff:76:24:2a:a4:62:13:3d:d3:b1:a5:a6:26:a2:
        11:66:13:1b:80:07:e9:ec:ee:c5:53:01:48:6f:b5:08:b2:9a:
        20:65:22:b1:3c:85:89:a7:18:8f:a3:74:dc:05:a9:9b:6d:5b:
        50:39:c3:51:5b:3e:6a:09:07:43:b2:52:36:c9:ac:aa:d2:7d:
        93:5e:81:f2:34:22:c4:1f:ca:e9:b0:94:55:20:b1:6c:83:48:
        dc:ec:16:85:ac:c9:c5:e3:ad:be:6a:34:9e:86:08:f5:d8:88:
        9d:35:e4:4d:e3:39:7e:12:83:5a:59:da:67:5a:77:6f:4a:90:
        04:92:ad:8f
SHA1 Fingerprint=41:4A:20:60:B7:38:C6:35:CC:7F:C2:43:E0:52:61:55:92:83:0C:53
```

```
-----BEGIN CERTIFICATE-----
MIIEXjCCA0agAwIBAgITB3MSSkvL1E7HtTvq8ZSELToPoTANBgkqhkiG9w0BAQsF
ADA5MQswCQYDVQQGEwJVUzEPMA0GA1UEChMGQW1hem9uMRkwFwYDVQQDExBBbWF6
b24gUm9vdCBDQSAxMB4XDTIyMDgyMzIyMjUzMFoXDTMwMDgyMzIyMjUzMFowPDEL
MAkGA1UEBhMCVVMxDzANBgNVBAoTBkFtYXpvbjEcMBoGA1UEAxMTQW1hem9uIFJT
QSAyMDQ4IE0wMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALtDGMZa
qHneKei1by6+pUPPLljTB143Si6VpEWPc6mSkFhZb/6qrkZyoHlQLbDYnI2D7hD0
sdzEqfnuAjIsuXQLG3A8TvX6V3oFNBFVe8NlLJHvBseKY88saLwufxkZVwk74g4n
WlNMXzla9Y5F3wwRHwMVH443xGz6UtGSZSqQ94eFx5X7Tlqt8whi8qCaKdZ5rNak
+r9nUThOeClqFd4oXych//Rc7Y0eX1KNWHYSI1Nk31mYgiK3JvH063g+K9tHA63Z
eTgKgndlh+WI+zv7i44HepRZjA1FYwYZ9Vv/9UkC5Yz8/yU65fgjaE+wVHM4e/Yy
C2osrPWE7gJ+dXMCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYD
VR0PAQH/BAQDAgGGMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAdBgNV
HQ4EFgQUwDFSzVpQw4J8dHHOy+mc+XrrguIwHwYDVR0jBBgwFoAUhBjMhTTsvAyU
lC4IWZzHshBOCggwewYIKwYBBQUHAQEEbzBtMC8GCCsGAQUFBzABhiNodHRwOi8v
b2NzcC5yb290Y2ExLmFtYXpvbnRydXN0LmNvbTA6BggrBgEFBQcwAoYuaHR0cDov
L2NydC5yb290Y2ExLmFtYXpvbnRydXN0LmNvbS9yb290Y2ExLmNlcjA/BgNVHR8E
ODA2MDSgMqAwhi5odHRwOi8vY3JsLnJvb3RjYTEuYW1hem9udHJ1c3QuY29tL3Jv
b3RjYTEuY3JsMBMGA1UdIAQMMAowCAYGZ4EMAQIBMA0GCSqGSIb3DQEBCwUAA4IB
AQAtTi6Fs0Azfi+iwm7jrz+CSxHH+uHl7Law3MQSXVtR8RV53PtR6r/6gNpqlzdo
Zq4FKbADi1v9Bun8RY8D51uedRfjsbeodizeBB8nXmeyD33Ep7VATj4ozcd31YFV
fgRhvTSxNrrTlNpWkUk0m3BMPv8sg381HhA6uEYokE5q9uws/3YkKqRiEz3TsaWm
JqIRZhMbgAfp7O7FUwFIb7UIspogZSKxPIWJpxiPo3TcBambbVtQOcNRWz5qCQdD
slI2yayq0n2TXoHyNCLEH8rpsJRVILFsg0jc7BaFrMnF462+ajSehgj12IidNeRN
4zl+EoNaWdpnWndvSpAEkq2P
-----END CERTIFICATE-----
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            06:7f:94:4a:2a:27:cd:f3:fa:c2:ae:2b:01:f9:08:ee:b9:c4:c6
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN = Starfield Services Root Certificate Author
        Validity
            Not Before: May 25 12:00:00 2015 GMT
            Not After : Dec 31 01:00:00 2037 GMT
        Subject: C = US, O = Amazon, CN = Amazon Root CA 1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b2:78:80:71:ca:78:d5:e3:71:af:47:80:50:74:
                    7d:6e:d8:d7:88:76:f4:99:68:f7:58:21:60:f9:74:
                    84:01:2f:ac:02:2d:86:d3:a0:43:7a:4e:b2:a4:d0:
                    36:ba:01:be:8d:db:48:c8:07:17:36:4c:f4:ee:88:
                    23:c7:3e:eb:37:f5:b5:19:f8:49:68:b0:de:d7:b9:
                    76:38:1d:61:9e:a4:fe:82:36:a5:e5:4a:56:e4:45:
                    e1:f9:fd:b4:16:fa:74:da:9c:9b:35:39:2f:fa:b0:
                    20:50:06:6c:7a:d0:80:b2:a6:f9:af:ec:47:19:8f:
                    50:38:07:dc:a2:87:39:58:f8:ba:d5:a9:f9:48:67:
                    30:96:ee:94:78:5e:6f:89:a3:51:c0:30:86:66:a1:
                    45:66:ba:54:eb:a3:c3:91:f9:48:dc:ff:d1:e8:30:
                    2d:7d:2d:74:70:35:d7:88:24:f7:9e:c4:59:6e:bb:
                    73:87:17:f2:32:46:28:b8:43:fa:b7:1d:aa:ca:b4:
                    f2:9f:24:0e:2d:4b:f7:71:5c:5e:69:ff:ea:95:02:
                    cb:38:8a:ae:50:38:6f:db:fb:2d:62:1b:c5:c7:1e:
                    54:e1:77:e0:67:c8:0f:9c:87:23:d6:3f:40:20:7f:
                    20:80:c4:80:4c:3e:3b:24:26:8e:04:ae:6c:9a:c8:
                    aa:0d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                84:18:CC:85:34:EC:BC:0C:94:94:2E:08:59:9C:C7:B2:10:4E:0A:08
            X509v3 Authority Key Identifier:
                9C:5F:00:DF:AA:01:D7:30:2B:38:88:A2:B8:6D:4A:9C:F2:11:91:83
            Authority Information Access:
                OCSP - URI:http://ocsp.rootg2.amazontrust.com
                CA Issuers - URI:http://crt.rootg2.amazontrust.com/rootg2.cer
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.rootg2.amazontrust.com/rootg2.crl
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        62:37:42:5c:bc:10:b5:3e:8b:2c:e9:0c:9b:6c:45:e2:07:00:
        7a:f9:c5:58:0b:b9:08:8c:3e:ed:b3:25:3c:b5:6f:50:e4:cd:
        35:6a:a7:93:34:96:32:21:a9:48:44:ab:9c:ed:3d:b4:aa:73:
        6d:e4:7f:16:80:89:6c:cf:28:03:18:83:47:79:a3:10:7e:30:
        5b:ac:3b:b0:60:e0:77:d4:08:a6:e1:1d:7c:5e:c0:bb:f9:9a:
        7b:22:9d:a7:00:09:7e:ac:46:17:83:dc:9c:26:57:99:30:39:
        62:96:8f:ed:da:de:aa:c5:cc:1b:3e:ca:43:68:6c:57:16:bc:
        d5:0e:20:2e:fe:ff:c2:6a:5d:2e:a0:4a:6d:14:58:87:94:e6:
        39:31:5f:7c:73:cb:90:88:6a:84:11:96:27:a6:ed:d9:81:46:
        a6:7e:a3:72:00:0a:52:3e:83:88:07:63:77:89:69:17:0f:39:
        85:d2:ab:08:45:4d:d0:51:3a:fd:5d:5d:37:64:4c:7e:30:b2:
        55:24:42:9d:36:b0:5d:9c:17:81:61:f1:ca:f9:10:02:24:ab:
        eb:0d:74:91:8d:7b:45:29:50:39:88:b2:a6:89:35:25:1e:14:
        6a:47:23:31:2f:5c:9a:fa:ad:9a:0e:62:51:a4:2a:a9:c4:f9:
        34:9d:21:18
SHA1 Fingerprint=06:B2:59:27:C4:2A:72:16:31:C1:EF:D9:43:1E:64:8F:A6:2E:1E:39
-----BEGIN CERTIFICATE-----
MIIEkjCCA3qgAwIBAgITBn+USionzfP6wq4rAfkI7rnExjANBgkqhkiG9w0BAQsF
```

```
ADCBmDELMAkGA1UEBhMCVVMxEDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTClNj
b3R0c2RhbGUxJTAjBgNVBAoTHFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4x
OzA5BgNVBAMTMlN0YXJmaWVsZCBTZXJ2aWNlcyBSb290IENlcnRpZmljYXRlIEF1
dGhvcml0eSAtIEcyMB4XDTE1MDUyNTEyMDAwMFoXDTM3MTIzMTAxMDAwMFowOTEL
MAkGA1UEBhMCVVMxDzANBgNVBAoTBkFtYXpvbjEZMBcGA1UEAxMQQW1hem9uIFJv
b3QgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALJ4gHHKeNXj
ca9HgFB0fW7Y14h29Jlo91ghYPl0hAEvrAIthtOgQ3pOsqTQNroBvo3bSMgHFzZM
9O6II8c+6zf1tRn4SWiw3te5djgdYZ6k/oI2peVKVuRF4fn9tBb6dNqcmzU5L/qw
IFAGbHrQgLKm+a/sRxmPUDgH3KKHOVj4utWp+UhnMJbulHheb4mjUcAwhmahRWa6
VOujw5H5SNz/0egwLX0tdHA114gk957EWW67c4cX8jJGKLhD+rcdqsq08p8kDi1L
93FcXmn/6pUCyziKrlA4b9v7LWIbxcceVOF34GfID5yHI9Y/QCB/IIDEgEw+OyQm
jgSubJrIqg0CAwEAAaOCATEwggEtMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/
BAQDAgGGMB0GA1UdDgQWBBSEGMyFNOy8DJSULghZnMeyEE4KCDAfBgNVHSMEGDAW
gBScXwDfqgHXMCs4iKK4bUqc8hGRgzB4BggrBgEFBQcBAQRsMGowLgYIKwYBBQUH
MAGGImh0dHA6Ly9vY3NwLnJvb3RnMi5hbWF6b250cnVzdC5jb20wOAYIKwYBBQUH
MAKGLGh0dHA6Ly9jcnQucm9vdGcyLmFtYXpvbnRydXN0LmNvbS9yb290ZzIuY2Vy
MD0GA1UdHwQ2MDQwMqAwoC6GLGh0dHA6Ly9jcmwucm9vdGcyLmFtYXpvbnRydXN0
LmNvbS9yb290ZzIuY3JsMBEGA1UdIAQKMAgwBgYEVR0gADANBgkqhkiG9w0BAQsF
AAOCAQEAYjdCXLwQtT6LLOkMm2xF4gcAevnFWAu5CIw+7bMlPLVvUOTNNWqnkzSW
MiGpSESrnO09tKpzbeR/FoCJbM8oAxiDR3mjEH4wW6w7sGDgd9QIpuEdfF7Au/ma
eyKdpwAJfqxGF4PcnCZXmTA5YpaP7dreqsXMGz7KQ2hsVxa81Q4gLv7/wmpdLqBK
bRRYh5TmOTFffHPLkIhqhBGWJ6bt2YFGpn6jcgAKUj6DiAdjd4lpFw85hdKrCEVN
0FE6/V1dN2RMfjCyVSRCnTawXZwXgWHxyvkQAiSr6w10kY17RSlQOYiypok1JR4U
akcjMS9cmvqtmg5iUaQqqcT5NJ0hGA==
-----END CERTIFICATE-----
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            a7:0e:4a:4c:34:82:b7:7f
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification Authority
        Validity
            Not Before: Sep  2 00:00:00 2009 GMT
            Not After : Jun 28 17:39:16 2034 GMT
        Subject: C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN = Starfield Services Root Certificate Autho
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d5:0c:3a:c4:2a:f9:4e:e2:f5:be:19:97:5f:8e:
                    88:53:b1:1f:3f:cb:cf:9f:20:13:6d:29:3a:c8:0f:
                    7d:3c:f7:6b:76:38:63:d9:36:60:a8:9b:5e:5c:00:
                    80:b2:2f:59:7f:f6:87:f9:25:43:86:e7:69:1b:52:
                    9a:90:e1:71:e3:d8:2d:0d:4e:6f:f6:c8:49:d9:b6:
                    f3:1a:56:ae:2b:b6:74:14:eb:cf:fb:26:e3:1a:ba:
                    1d:96:2e:6a:3b:58:94:89:47:56:ff:25:a0:93:70:
                    53:83:da:84:74:14:c3:67:9e:04:68:3a:df:8e:40:
                    5a:1d:4a:4e:cf:43:91:3b:e7:56:d6:00:70:cb:52:
                    ee:7b:7d:ae:3a:e7:bc:31:f9:45:f6:c2:60:cf:13:
                    59:02:2b:80:cc:34:47:df:b9:de:90:65:6d:02:cf:
                    2c:91:a6:a6:e7:de:85:18:49:7c:66:4e:a3:3a:6d:
                    a9:b5:ee:34:2e:ba:0d:03:b8:33:df:47:eb:b1:6b:
                    8d:25:d9:9b:ce:81:d1:45:46:32:96:70:87:de:02:
                    0e:49:43:85:b6:6c:73:bb:64:ea:61:41:ac:c9:d4:
                    54:df:87:2f:c7:22:b2:26:cc:9f:59:54:68:9f:fc:
                    be:2a:2f:c4:55:1c:75:40:60:17:85:02:55:39:8b:
                    7f:05
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                9C:5F:00:DF:AA:01:D7:30:2B:38:88:A2:B8:6D:4A:9C:F2:11:91:83
            X509v3 Authority Key Identifier:
                BF:5F:B7:D1:CE:DD:1F:86:F4:5B:55:AC:DC:D7:10:C2:0E:A9:88:E7
            Authority Information Access:
                OCSP - URI:http://o.ss2.us/
                CA Issuers - URI:http://x.ss2.us/x.cer
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://s.ss2.us/r.crl
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        23:1d:e3:8a:57:ca:7d:e9:17:79:4c:f1:1e:55:fd:cc:53:6e:
        3e:47:0f:df:c6:55:f2:b2:04:36:ed:80:1f:53:c4:5d:34:28:
        6b:be:c7:55:fc:67:ea:cb:3f:7f:90:b2:33:cd:1b:58:10:82:
        02:f8:f8:2f:f5:13:60:d4:05:ce:f1:81:08:c1:dd:a7:75:97:
        4f:18:b9:6d:de:f7:93:91:08:ba:7e:40:2c:ed:c1:ea:bb:76:
        9e:33:06:77:1d:0d:08:7f:53:dd:1b:64:ab:82:27:f1:69:d5:
        4d:5e:ae:f4:a1:c3:75:a7:58:44:2d:f2:3c:70:98:ac:ba:69:
        b6:95:77:7f:0f:31:5e:2c:fc:a0:87:3a:47:69:f0:79:5f:f4:
        14:54:a4:95:5e:11:78:12:60:27:ce:9f:c2:77:ff:23:53:77:
        5d:ba:ff:ea:59:e7:db:cf:af:92:96:ef:24:9a:35:10:7a:9c:
        91:c6:0e:7d:99:f6:3f:19:df:f5:72:54:e1:15:a9:07:59:7b:
        83:bf:52:2e:46:8c:b2:00:64:76:1c:48:d3:d8:79:e8:6e:56:
        cc:ae:2c:03:90:d7:19:38:99:e4:ca:09:19:5b:ff:07:96:b0:
        a8:7f:34:49:df:56:a9:f7:b0:5f:ed:33:ed:8c:47:b7:30:03:
        5d:f4:03:8c
SHA1 Fingerprint=9E:99:A4:8A:99:60:B1:49:26:BB:7F:3B:02:E2:2D:A2:B0:AB:72:80
-----BEGIN CERTIFICATE-----
MIIEdTCCA12gAwIBAgIJAKcOSkw0grd/MA0GCSqGSIb3DQEBCwUAMGgxCzAJBgNV
BAYTAlVTMSUwIwYDVQQKExxTdGFyZmllbGQgVGVjaG5vbG9naWVzLCBJbmMuMTIw
```

```
MAYDVQQLEylTdGFyZmllbGQgQ2xhc3MgMiBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0
eTAeFw0wOTA5MDIwMDAwMDBaFw0zNDA2MjgxNzM5MTZaMIGYMQswCQYDVQQGEwJV
UzEQMA4GA1UECBMHQXJpem9uYTETMBEGA1UEBxMKU2NvdHRzZGFsZTElMCMGA1UE
ChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLjE7MDkGA1UEAxMyU3RhcmZp
ZWxkIFNlcnZpY2VzIFJvb3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVDDrEKvlO4vW+GZdfjohTsR8/
y8+fIBNtKTrID30892t2OGPZNmCom15cAICyL1l/9of5JUOG52kbUpqQ4XHj2C0N
Tm/2yEnZtvMaVq4rtnQU68/7JuMauh2WLmo7WJSJR1b/JaCTcFOD2oR0FMNnngRo
Ot+OQFodSk7PQ5E751bWAHDLUu57fa4657wx+UX2wmDPE1kCK4DMNEffud6QZW0C
zyyRpqbn3oUYSXxmTqM6bam17jQuug0DuDPfR+uxa40l2ZvOgdFFRjKWcIfeAg5J
Q4W2bHO7ZOphQazJ1FTfhy/HIrImzJ9ZVGif/L4qL8RVHHVAYBeFAlU5i38FAgMB
AAGjgfAwge0wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAYYwHQYDVR0O
BBYEFJxfAN+qAdcwKziIorhtSpzyEZGDMB8GA1UdIwQYMBaAFL9ft9HO3R+G9FtV
rNzXEMIOqYjnME8GCCsGAQUFBwEBBEMwQTAcBggrBgEFBQcwAYYQaHR0cDovL28u
c3MyLnVzLzAhBggrBgEFBQcwAoYVaHR0cDovL3guc3MyLnVzL3guY2VyMCYGA1Ud
HwQfMB0wG6AZoBeGFWh0dHA6Ly9zLnNzMi51cy9yLmNybDARBgNVHSAECjAIMAYG
BFUdIAAwDQYJKoZIhvcNAQELBQADggEBACMd44pXyn3pF3lM8R5V/cxTbj5HD9/G
VfKyBDbtgB9TxF00KGu+x1X8Z+rLP3+QsjPNG1gQggL4+C/1E2DUBc7xgQjB3ad1
l08YuW3e95ORCLp+QCztweq7dp4zBncdDQh/U90bZKuCJ/Fp1U1ervShw3WnWEQt
8jxwmKy6abaVd38PMV4s/KCHOkdp8Hlf9BRUpJVeEXgSYCfOn8J3/yNTd126/+pZ
59vPr5KW7ySaNRB6nJHGDn2Z9j8Z3/VyVOEVqQdZe4O/Ui5GjLIAZHYcSNPYeehu
VsyuLAOQ1xk4meTKCRlb/weWsKh/NEnfVqn3sF/tM+2MR7cwA130A4w=
-----END CERTIFICATE-----
```

2.2. Online Certificate Status Protocol (OCSP)

The Online Certificate Status check protocol makes revocation checks faster and simpler than downloading a full certificate revocation list, but at the cost of privacy, and of requiring the client to connect to a second server before they can continue with their request. How could this be fixed to provide the best of both worlds?

2.3. Certificate Transparency

How does Certificate Transparency improve security? Who can benefit from monitoring the logs, and what should they look for?