BNSS: Cryptography, PKI, and Kerberos

EP2520: Building Networked Systems Security

Networked Systems Security Group, www.eecs.kth.se/nss

P. Papadimitratos

January 22, 2021

Contents

Cryptographic primitives

Symmetric key cryptography
Asymmetric key cryptography
Digital signatures

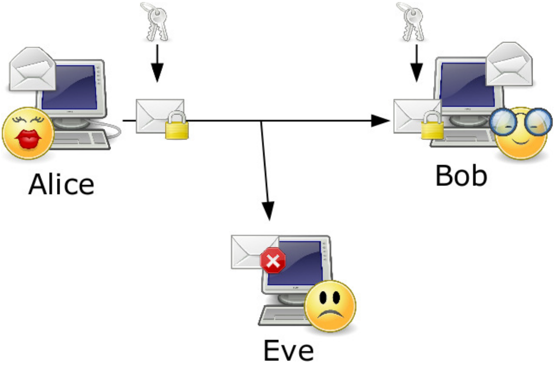
Public Key Infrastructure

Certificates
X.509

Kerberos

Software

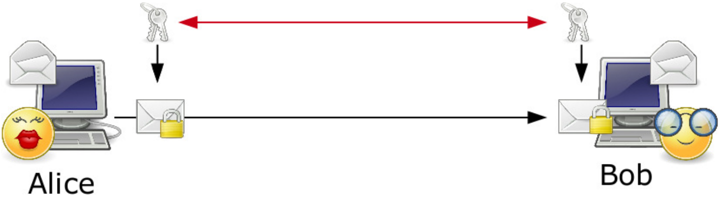
Cryptography



- Kerckhoffs's principle: *"The enemy knows the crypto-system"*
- The cryptographic secret or private keys must be kept secret

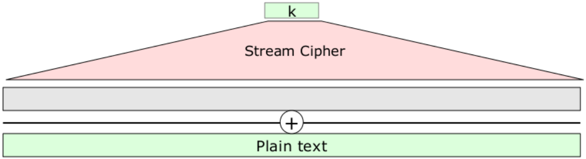
Symmetric key crypto

- Same key to encrypt and decrypt
- Computationally efficient

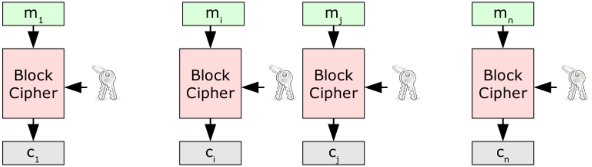


Types of ciphers

- Stream ciphers (Wikipedia, Book Chapter)
  - RC4
  - A5/1



- Block ciphers (Wikipedia, Book)
  - DES
  - AES

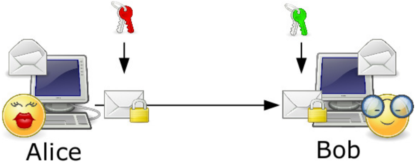


Symmetric Key Standards

- Data Encryption Standard (DES)
- Triple Data Encryption Algorithm (TDEA)
- Advanced Encryption Standard (AES)
- Rivest Cipher 4 (RC4)
- International Data Encryption Algorithm (IDEA)
- Camellia

Asymmetric key crypto

- Two different keys
  - One public
  - One private



- Alice encrypts the message with Bob's public key
- Bob decrypts it with his private key

- Infeasible to obtain the private key
  - From the ciphertext
  - From the public key

- Computationally less efficient than symmetric key encryption

Asymmetric key crypto cont'd

- Based on computationally hard problems
- Integer factorization
  - Given n, the product of two primes, p and q, it is hard to find p, q.
  - RSA
- Discrete logarithm
  - Given g and $y = g^x$ is hard to find x in modulo p prime
  - ElGamal

Asymmetric key crypto cont'd

- Rivest, Shamir, Adleman algorithm (RSA)
- Digital Signature Algorithm (DSA)
- Elliptic Curve DSA (ECDSA)
- ElGamal

Digital signatures

- Digital signature generation and verification
  - Use the private key to sign the message
  - Use the public key to verify the message signature

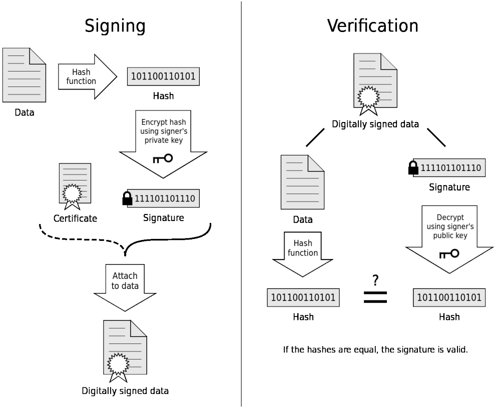


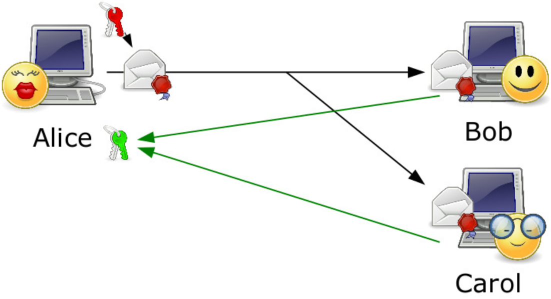
Figure: Source wikipedia.org

- Rather than signing (encrypting) the entire message, sign only the message hash/digest
- What binds the public key to the signer?

Digital signatures cont'd

Anyone with the signer's certificate/public key can verify a signature

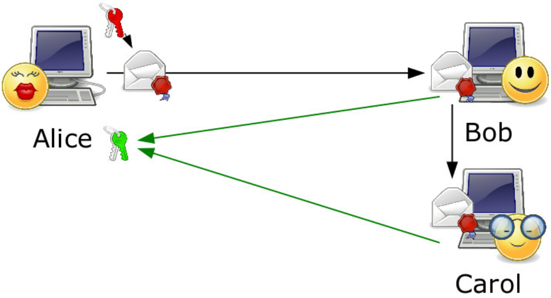
- Unlike the need to have a shared key with each and every entity



Digital signatures cont'd

Transferable

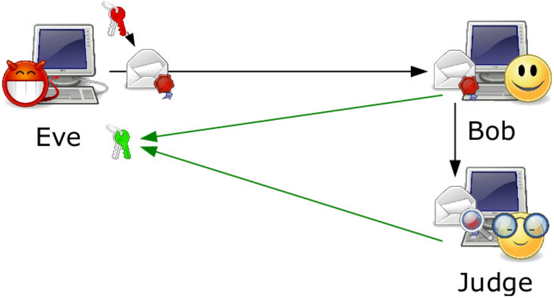
- The signature travels with the message
- A third entity can always authenticate the original message



Digital signatures cont'd

Non-repudiable

- Nobody can manipulate a signed message undetected, or produce a valid signature without the signer's private key

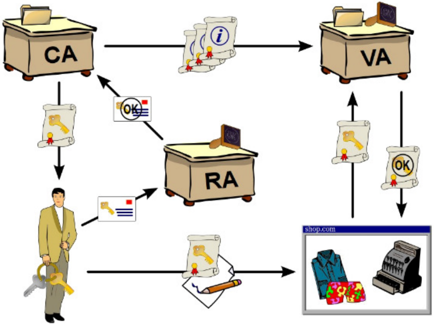


Public Key Infrastructures (PKIs)

- To authenticate hosts over open networks
  - Beyond local area networks
  - Passwords could be inconvenient and easy to steal
- Need to distribute public keys
  - Who is who?

PKIs

- Constituent parts
  - Hardware & Software
  - People & Policies
  - Procedures
- Use
  - Management of credentials: provision of certificates, revocation of certificates
- Applications
  - E-commerce
  - E-banking



Certificates

- Bind the public key to (the identity of) an entity (company, institution, individual, machine, service)
  - Digital signature from a trusted third party, the Certification Authority (CA)
- The CA has a certificate itself
- Hierarchical structure, root CAs and root certificates; PKI
- X.509 Standard (PKIX)

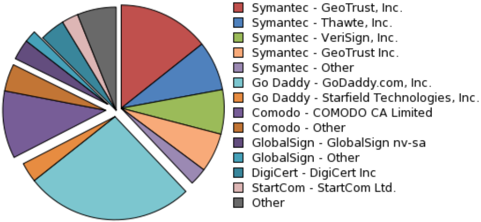


Figure: Market share of CAs (soucre link))

Chain or Web of Trust

- Certificate Chain

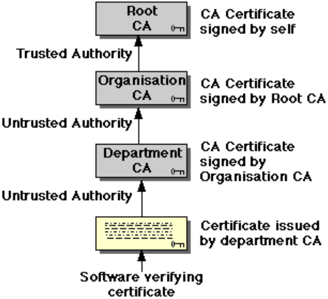
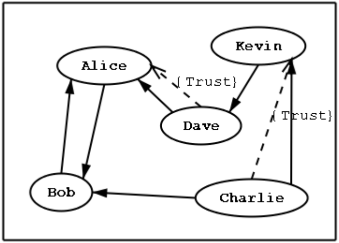

Root CA
CA Certificate signed by self
Trusted Authority
Organisation CA
CA Certificate signed by Root CA
Untrusted Authority
Department CA
CA Certificate signed by Organisation CA
Untrusted Authority
Certificate issued by department CA
Software verifying certificate

Figure: Source latrobe.edu.au

- Web of Trust (Pretty Good Privacy (PGP))



An example of the web of trust model

Figure: Source gnu.org

Certificate Revocation

When to revoke:

- Certificates can cease to be valid for various reasons, e.g.,
- Entity must be evicted from the system
- Its private key is compromised

How to revoke:

- Certificate Revocation List (CRL) RFC 1422
- Δ-CRL (incremental CRL) RFC 2459
- Online Certificate Status Protocol (OCSP) RFC 2560

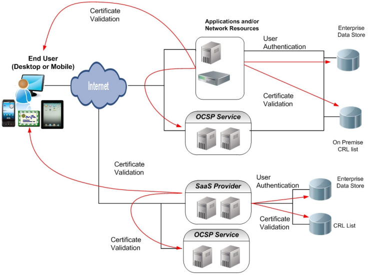


Figure: Source gosecureauth.com

X.509

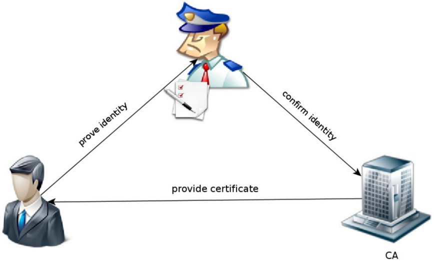
Public Key Infrastructure (PKIX - RFC 4158) standard

- Public Key Infrastructure (PKI)
- Privilege Management Infrastructure (PMI)

X.509 specifies

- Certificates
- Certificate revocation lists
- Attribute certificates
- Certification path validation algorithm

PKIX overview



Encrypted with CA's private key

version	Serial number	algorithm	issuer	Validity period	...	Properties

X.509 Format

Every X.509 certificate has

- Data section

- Signature section

Data Section

```
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 7829 (0x1e95)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting
           cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Jul  9 16:04:02 1998 GMT
           Not After : Jul  9 16:04:02 1999 GMT
       Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                OU=FreeSoft, CN=www.freesoft.org/emailAddress=
                    baccala@freesoft.org
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                   33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                   66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                   70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                   16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                   c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                   8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                   d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                   e8:35:1c:9e:27:52:7e:41:8f
               Exponent: 65537 (0x10001)
```

Signature Section

```
   Signature Algorithm: md5WithRSAEncryption
       93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
       92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
       ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
       d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
       0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
       5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
       8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
       68:9f
```

X.509 Format: Data Section

Data Section

```
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 7829 (0x1e95)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting
           cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Jul  9 16:04:02 1998 GMT
           Not After : Jul  9 16:04:02 1999 GMT
       Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                OU=FreeSoft, CN=www.freesoft.org/emailAddress=
                    baccala@freesoft.org
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                   33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                   66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                   70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                   16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                   c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                   8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                   d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                   e8:35:1c:9e:27:52:7e:41:8f
               Exponent: 65537 (0x10001)
```

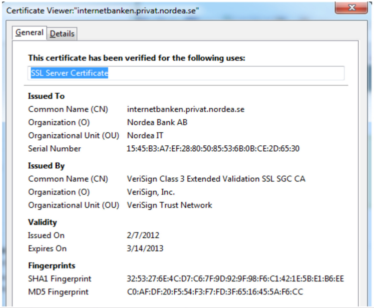
X.509 Format: Signature Section

Signature Section

```
Signature Algorithm: md5WithRSAEncryption
    93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
    92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
    ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
    d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
    0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
    5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
    8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
    68:9f
```

TLS/SSL Certificates

- Widely used in Internet
  - Secure client/server applications
  - Web browsers with root certificates pre-stored



This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	internetbanken.privat.nordea.se
Organization (O)	Nordea Bank AB
Organizational Unit (OU)	Nordea IT
Serial Number	15:45:B3:A7:EF:28:80:50:85:53:6B:0B:CE:2D:65:30

Issued By

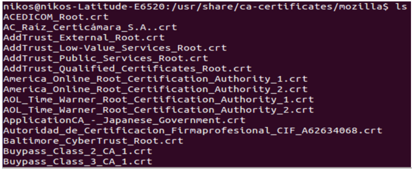
Common Name (CN)	VeriSign Class 3 Extended Validation SSL SGC CA
Organization (O)	VeriSign, Inc.
Organizational Unit (OU)	VeriSign Trust Network

Validity

Issued On	2/7/2012
Expires On	3/14/2013

Fingerprints

SHA1 Fingerprint	32:53:27:6E:4C:D7:C6:7F:9D:92:9F:98:F6:C1:42:1E:5B:E1:B6:EE
MD5 Fingerprint	C0:AF:DF:20:F5:54:F3:F7:FD:3F:65:16:45:5A:F6:CC



```
nikos@nikos-Latitude-E6520:/usr/share/ca-certificates/mozilla$ ls
ACEDICOM_Root.crt
AC_Raíz_Certicámara_S.A..crt
AddTrust_External_Root.crt
AddTrust_Low-Value_Services_Root.crt
AddTrust_Public_Services_Root.crt
AddTrust_Qualified_Certificates_Root.crt
America_Online_Root_Certification_Authority_1.crt
America_Online_Root_Certification_Authority_2.crt
AOL_Time_Warner_Root_Certification_Authority_1.crt
AOL_Time_Warner_Root_Certification_Authority_2.crt
ApplicationCA_-_Japanese_Government.crt
Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt
Baltimore_CyberTrust_Root.crt
Buypass_Class_2_CA_1.crt
Buypass_Class_3_CA_1.crt
```

X.509 Certificate Revocation List

RFC 3280 defines two states

- Revoked
- On hold (reversible state, suspsension)

Revoke a certificate because, e.g., RFC 5280

- unspecified (0)
- keyCompromise (1)
- cACompromise (2)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)
- certificateHold (6)
- (value 7 is not used)
- removeFromCRL (8)
- privilegeWithdrawn (9)
- aACompromise (10)

X.509 CRL format

Certificate Revocation List

```
Certificate Revocation List:
    Data:
        Version:  v2
        Signature Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5
        Issuer: CN=Certificate Authority,O=Example Domain
        This Update: Wednesday, July 29, 2009 8:59:48 AM GMT-08:00
        Next Update: Friday, July 31, 2009 8:59:48 AM GMT-08:00
        Revoked Certificates: 1-3 of 3
            Serial Number: 0x11
            Revocation Date: Thursday, July 23, 2009 10:07:15 AM GMT
                -08:00
            Extensions:
                Identifier: Revocation Reason - 2.5.29.21
                    Critical: no
                    Reason: Privilege_Withdrawn
            Serial Number: 0x1A
            Revocation Date: Wednesday, July 29, 2009 8:50:11 AM GMT
                -08:00
            Extensions:
                Identifier: Revocation Reason - 2.5.29.21
                    Critical: no
                    Reason: Certificate_Hold
                Identifier: Invalidity Date - 2.5.29.24
                    Critical: no
                    Invalidity Date: Sun Jul 26 23:00:00 GMT-08:00 2009
            Serial Number: 0x19
            Revocation Date: Wednesday, July 29, 2009 8:50:49 AM GMT
                -08:00
            Extensions:
                Identifier: Revocation Reason - 2.5.29.21
                    Critical: no
                    Reason: Key_Compromise
                Identifier: Invalidity Date - 2.5.29.24
                    Critical: no
                    Invalidity Date: Fri Jul 24 23:00:00 GMT-08:00 2009
    Signature:
        Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5
        Signature:
            47:D2:CD:C9:E5:F5:9D:56:0A:97:31:F5:D5:F2:51:EB:
            1F:CF:FA:9E:63:D4:80:13:85:E5:D8:27:F0:69:67:B5:
            89:4F:59:5E:69:E4:39:93:61:F2:E3:83:51:0B:68:26:
            CD:99:C4:A2:6C:2B:06:43:35:36:38:07:34:E4:93:80:
            99:2F:79:FB:76:E8:3D:4C:15:5A:79:4E:E5:3F:7E:FC:
            D8:78:0D:1D:59:A0:4C:14:42:B7:22:92:89:38:3A:4C:
            4A:3A:06:DE:13:74:0E:E9:63:74:D0:2F:46:A1:03:37:
            92:F0:93:D9:AA:F8:13:C5:06:25:02:B0:FD:3B:41:E7:
            62:6F:67:A3:9F:F5:FA:03:41:DA:8D:FD:EA:2F:E3:2B:
            3E:F8:E9:CC:3B:9F:E4:ED:73:F2:9E:B9:54:14:C1:34:
            68:A7:33:8F:AF:38:85:82:40:A2:06:97:3C:B4:88:43:
            7B:AF:5D:87:C4:47:63:4A:11:65:E3:75:55:4D:98:97:
            C2:2E:62:08:A4:04:35:5A:FE:0A:5A:6E:F1:DE:8E:15:
            27:1E:0F:87:33:14:16:2E:57:F7:DC:77:BE:D2:75:AB:
            A9:7C:42:1F:84:6D:40:EC:E7:ED:84:F8:14:16:28:33:
            FD:11:CD:C5:FC:49:B7:7B:39:57:B3:E6:36:E5:CD:B6
```

X.509 CRL format

```
Revoked Certificates: 1-3 of 3
    Serial Number: 0x11
    Revocation Date: Thursday, July 23, 2009 10:07:15 AM GMT
        -08:00
    Extensions:
        Identifier: Revocation Reason - 2.5.29.21
            Critical: no
            Reason: Privilege_Withdrawn
    Serial Number: 0x1A
    Revocation Date: Wednesday, July 29, 2009 8:50:11 AM GMT
        -08:00
    Extensions:
        Identifier: Revocation Reason - 2.5.29.21
            Critical: no
            Reason: Certificate_Hold
        Identifier: Invalidity Date - 2.5.29.24
            Critical: no
            Invalidity Date: Sun Jul 26 23:00:00 GMT-08:00 200
    Serial Number: 0x19
    Revocation Date: Wednesday, July 29, 2009 8:50:49 AM GMT
        -08:00
```

X.509 CRL format

```
Signature:
    Algorithm: SHA1withRSA - 1.2.840.113549.1.1.5
    Signature:
        47:D2:CD:C9:E5:F5:9D:56:0A:97:31:F5:D5:F2:51:EB:
        1F:CF:FA:9E:63:D4:80:13:85:E5:D8:27:F0:69:67:B5:
        89:4F:59:5E:69:E4:39:93:61:F2:E3:83:51:0B:68:26:
        CD:99:C4:A2:6C:2B:06:43:35:36:38:07:34:E4:93:80:
        99:2F:79:FB:76:E8:3D:4C:15:5A:79:4E:E5:3F:7E:FC:
        D8:78:0D:1D:59:A0:4C:14:42:B7:22:92:89:38:3A:4C:
        4A:3A:06:DE:13:74:0E:E9:63:74:D0:2F:46:A1:03:37:
        92:F0:93:D9:AA:F8:13:C5:06:25:02:B0:FD:3B:41:E7:
        62:6F:67:A3:9F:F5:FA:03:41:DA:8D:FD:EA:2F:E3:2B:
        3E:F8:E9:CC:3B:9F:E4:ED:73:F2:9E:B9:54:14:C1:34:
        68:A7:33:8F:AF:38:85:82:40:A2:06:97:3C:B4:88:43:
        7B:AF:5D:87:C4:47:63:4A:11:65:E3:75:55:4D:98:97:
        C2:2E:62:08:A4:04:35:5A:FE:0A:5A:6E:F1:DE:8E:15:
        27:1E:0F:87:33:14:16:2E:57:F7:DC:77:BE:D2:75:AB:
        A9:7C:42:1F:84:6D:40:EC:E7:ED:84:F8:14:16:28:33:
        FD:11:CD:C5:FC:49:B7:7B:39:57:B3:E6:36:E5:CD:B6
```

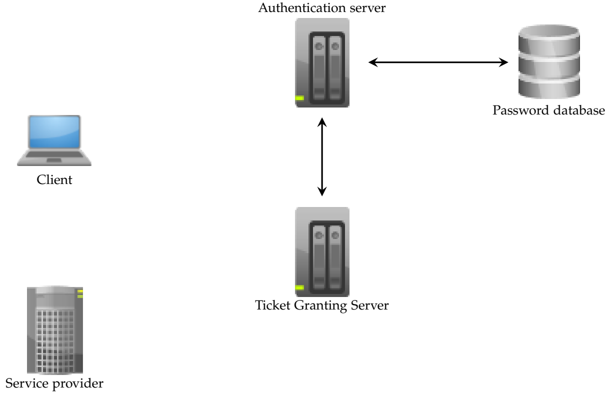
Kerberos

Authenticating users in local area networks without PKIs

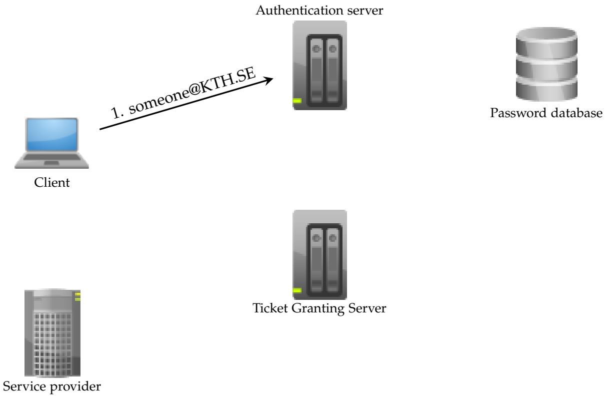
Kerberos cont'd

- Network authentication protocol for client/server applications
- Developed at MIT in the mid 1980s
- Untrusted network and trusted hosts
- RFC 4120
- Access to services
  - e.g., mail servers, file servers
- Kerberos 5 is the main version in use
- Why use Kerberos?
  - PKIs, certificates, cost

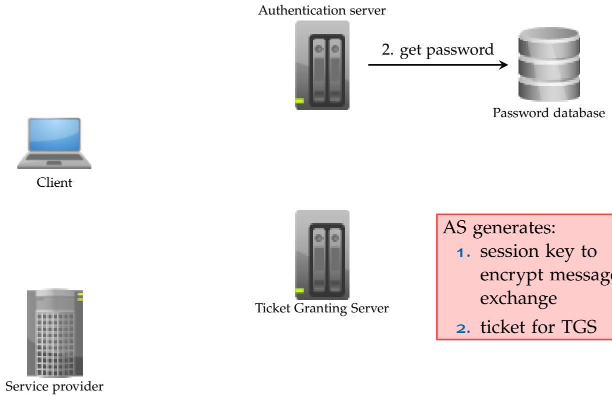
Kerberos cont'd



Kerberos cont'd



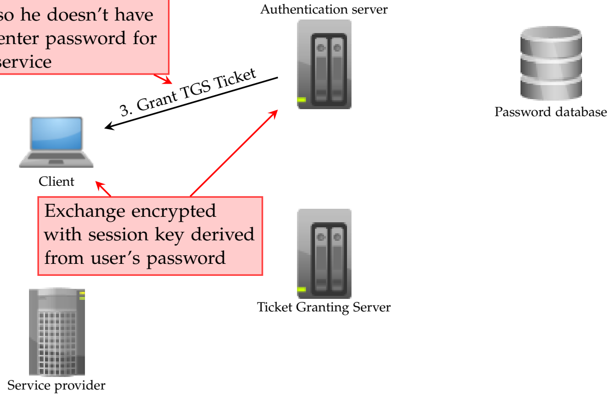
Kerberos cont'd



AS generates:

1. session key to encrypt message exchange
2. ticket for TGS

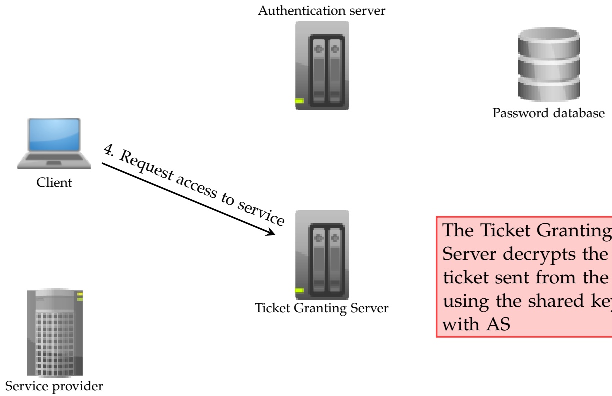
Kerberos cont'd



User obtains TGS ticket once so he doesn't have to re-enter password for each service

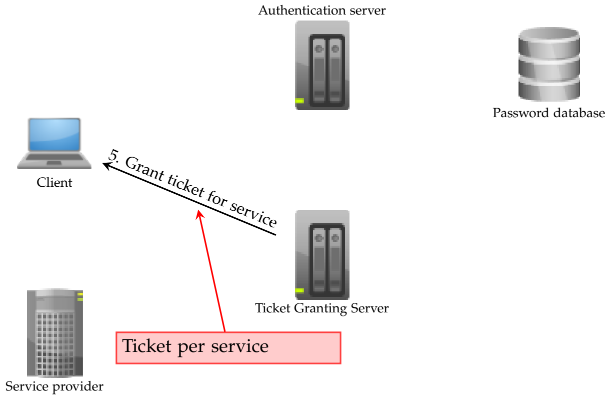
Exchange encrypted with session key derived from user's password

Kerberos cont'd



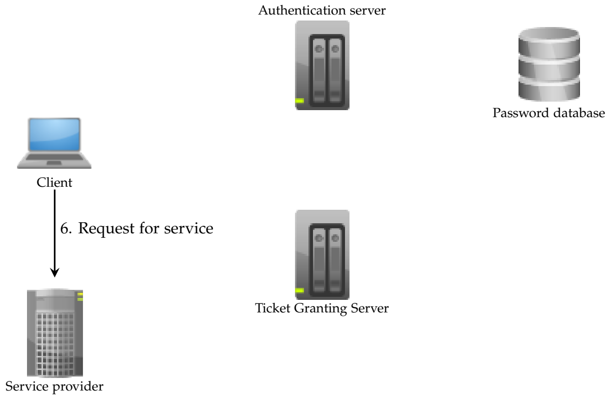
The Ticket Granting Server decrypts the TGS ticket sent from the user using the shared key with AS

Kerberos cont'd

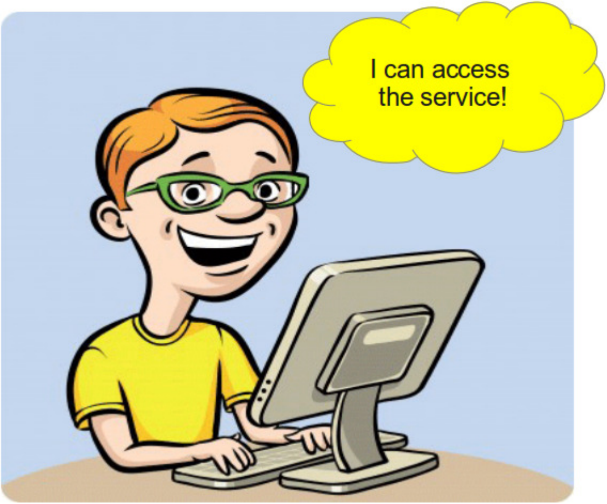


Ticket per service

Kerberos cont'd



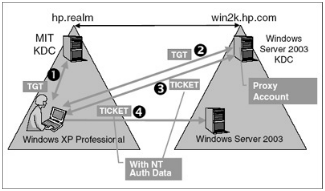
Final result



Kerberos cont'd

Multiple Realms

- Supports inter-realm Kerberos communication
- Requires trust between Kerberos servers
- Users authenticated in their realm
- Access services in neighboring realms



Kerberos recap

- Untrusted network but trusted hosts
  - How can hosts be reliable? Software running on hosts?
  - If hosts are compromised, is Kerberos compromised?
- Kerberos 5 brings a lot of improvements to Kerberos 4
  - Stronger cryptography
- Password based security is a weakness point
- Suitable for local area or neighboring networks (Multiple Realm Kerberos)
- Alternative to certificates and costly PKIs

Software

Cryptography

- OpenSSL
- GnuTLS

Public Key Infrastructure

- OpenCA
- EJBCA

Kerberos

- MIT Kerberos
- Heimdal