On the Uses of Cryptography in Industry

Hamdi Murat Yıldırım

Bilkent Üniversitesi,
Bilgisayar Teknolojisi ve Bilişim Sistemleri Bölümü

hmurat@bilkent.edu.tr hmurat.bilkent.edu.tr

27 December 2014

"IAM Alumni Meeting: Workshop on Cryptography and Applications"
METU, IAM CRYPTO LAB

Outline

- Information Security Goals
- Cryptographic Primitivies
- Kerboros
- X.509 Authentication Service
- Public-Key Infrastructure (PKI)
- Secure/Multipurpose Internet Mail Extension (S/MIME)
- Turkish Electronic Signature Law
- TCP/IP Layers and Protocols
- Transport Layer Security (TLS)
- SSH
- IPSEC
- Use of Cryptography in Wireless Communications
- A study about improper use of Cryptography in Mobile Applications
- Online Payment
- Cryptographic Module Validation Program (CMVP) and FIPS 140-2
- Hardware Security Modules (HSM)
- Lightweight Cryptography
- Some issues in Cloud Computing Security
- Data Security in the Cloud
- Remarks

Information Security Goals

- **Information security,** sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical)**.**
- **Classic InfoSec triad —** confidentiality, integrity and availability
- **Information Assurance and Security (IAS) literature —**

  Confidentiality, Integrity, Availability, Accountability, Auditability, Authenticity/Trustworthiness, Non-repudiation and Privacy.

Information Security Goals

- **Confidentiality** The process of and obligation to keep a transaction, documents, etc., private and secret, i.e., confidential; the right to withhold information, e.g. medical information, from others.
- **Integrity** data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle, i.e., data cannot be modified in an unauthorized or undetected manner.
- **Availability** for any information system to serve its purpose, the information must be available when it is needed.
- **Authenticity** it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine.
- **Non-repudiation** In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.
- **Accountability** the security goal that generates the requirement for actions of an entity to be traced uniquely. Tracing security breaches.
- **Anonymity** Maintaining user anonymity is desirable in a variety of electronic commerce applications.

Cryptographic Primitivies

- Symmetric Encryption (SE): ensuring confidentiality, integrity *, authenticity *
- Asymmetric Encryption (AE): Ensuring confidentiality, integrity, authenticity, non-repudiation, key exchange
- Cryptographic Hash Functions (CHF) : integrity
- SE & CHF ; Message Authentication Code (MAC) algorithms: integrity and authenticity
- AE; CHF: ensuring anonymity
  - Group blind digital signatures
  - Freenet: A distributed anonymous information storage and retrieval system
  - Onion routing
  - a limited form of anonymity provided by UMTS/LTE protocol for mobile phone networks

(*) with the use of suitable block modes of operation.

Cryptographic Protocols

- A security protocol (cryptographic protocol or encryption protocol) is an abstract or concrete protocol that performs a security-related function and applies cryptographic methods, often as sequences of cryptographic primitives
- Cryptographic protocols are widely used for secure application-level data transport. A cryptographic protocol usually incorporates at least some of these aspects:
  - **Key agreement or establishment**

    Protocols: NIST Special Publication 800-56A and 800-56B; ANSI X9.42 and X9.63; ISO/IEC 11770-2,-3 and -4;
  - **Entity authentication**

    Protocols: ISO/IEC 9798-1,-2,-3,-4,-5 and-6
  - **Symmetric encryption and message authentication material construction**

    Protocol: ISO 16609:2012
  - **Secured application-level data transport**
  - **Non-repudiation methods**
  - **Secret sharing methods**
  - **Secure multi-party computation**

Kerboros

(Ref. http://en.wikipedia.org/wiki/Kerberos_%28protocol%29)

- “ ... Kerberos builds on ***symmetric key cryptography*** and requires a trusted third party, and optionally may use ***public-key cryptography*** during certain phases of authentication. ..”
- " ... Windows 2000 and later uses Kerberos as its default authentication method”.

“ .. In general, joining a client to a Windows domain means enabling Kerberos as default protocol for authentications from that client to services in the Windows domain ...”

“ .. Many UNIX and UNIX-like operating systems, including FreeBSD, Apple's Mac OS X, Red Hat Enterprise Linux, Oracle's Solaris, IBM's AIX and Z/OS, HP's OpenVMS and others, include software for Kerberos authentication of users or services ..”

- Version 5 block ciphers: DES, 3DES, AES or Camellia

X.509 Authentication Service

- X.509 is part of X.500 series which defines a directory service
- 1988, V2-1993, V3-1995
- Based on public-key cryptography and digital signatures
- Defines a framework for the provision of authentication services
- Repository of public key certificates
- Used in S/MIME, IPSec, SSL and SET

X.509 Authentication Service

- Distributed set of servers that maintains a database about users.
- Each certificate contains the *public key of a user* and is signed with the *private key of a trusted certification authority (CA).*
- *A certificate is associated with each user*
- Is used in S/MIME, IP Security, SSL/TLS and SET.

Public-Key Infrastructure (PKI)

RFC 2822 define Public-Key Infrastructure (PKI) as the set of hardware, software, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.

Main objectives for developing **PKI** is to enable Secure, convenient and efficient obtaining of public keys.

IETF PKI X.509 **(PKIX)** working group (http://www.ietf.org/html.charters/pkix-charter.html) setting up a formal (and generic) model based on X.509 in order to use PKI architecture on the Internet.

Turkish Electronic Signature Law / Qualified Electronic Certificate Service Providers

- Turkish Electronic Signature Law (Elektronik imza Kanunu)

  http://www.resmigazete.gov.tr/eskiler/2004/01/20040123.htm#1

- Qualified Electronic Certificate Service Providers (Nitelikli (yasal gerçerliliği olan) Elektronik İmza Hizmet Sağlayıcılar):
  - http://www.turktrust.com.tr/en/index.html
  - http://www.e-guven.com/en/about_E-GUVEN.html
  - http://e-tugra.com.tr
  - http://www.kamusm.gov.tr/
  - http://www.egmsm.gov.tr
- Mobile Signature (All GSM operators in Turkey)
- Registered Electronic Mail in Turkey (Qualified providers: PTT, TNB, TÜRKKEP, INTERKEP) / legislation issues

Protocols use X.509

- Electronic Signature and Mobil Signature
- Registered, Certified Email Protocols
- S/MIME
- TLS
  - Many Application layer protocols use TLS

TCP/IP Layers and Protocols

Application Layer: HTTP, SMTP, DNS, IMAP, DHCP, IMAP, IRC,
Transport Layer: TCP and UDP
Internetwork Layer: IPv4 and IPv6
Network Access Layer: Ethernet

Secure/Multipurpose Internet Mail Extension (S/MIME)

RFCs 5751 (proposed for version 3.2), 3370, 3850, 3851, 3852

- S/MIME (high industry interest due to X.509 certificates use) provides the following cryptographic security services for electronic messaging applications:
  - authentication,
  - message integrity,
  - non-repudiation of origin (using digital signatures),
  - privacy and data security (using encryption).
- S/MIME uses
  - symmetric ciphers,
  - public key cryptography,
  - hashing, and public key certificates.
- Supported by MS Outlook Exp., Mozilla Thunderbird
- Personal use alternative PGP (Standard: Openpgp)

Transport Layer Security (TLS)

- Transport Layer Security (TLS) is a cryptographic protocol
  - usually implemented on top of any of the Transport Layer protocols, encapsulating the application-specific protocols such as

    HTTP, IRC, FTP, SMTP, IMAP, POP, NNTP and **XMPP**

    Eg. HTTPS: HTTP over SSL/TLS ; SMTPS: SMTP (e-mail) over SSL/TLS
  - entity authentication mechanism, based on the **X.509 system**;
  - a key setup phase, where a symmetric encryption key is shared/formed by employing public-key cryptography (*RSA-PKCS#1-v1.5*, *Diffie-Hellman key exchange*); and an application-level data transport function.
  - uses HMAC for MAC
  - Some TLS implementations (GnuTLS, Openssl, LibreSSL, PolarSSL, Bouncy Castle, Botan, CyaSSL)
  - OpenSSL and FIPS 140-2 Validation Status
  - Video: Using SSL/TLS **More videos and materials available from SecAppDev Course (aiming to broaden security awareness in the development community and advance secure software engineering practices)**

OPENSSL

- The OpenSSL Project is a Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols as well as a full-strength general purpose cryptography library.
- OpenSSL vulnerabilities exist
- CVE-2014-0160: 7th April 2014

“ .. A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64kB of memory to a connected client or server (a.k.a. Heartbleed). This issue did not affect versions of OpenSSL prior to 1.0.1. Fixed in OpenSSL 1.0.1g (Affected 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1) ..”

- “ ... At the time of disclosure, some 17% (around half a million) of the Internet's secure web servers certified by trusted authorities were believed to be vulnerable to the attack, allowing theft of the servers' private keys and users' session cookies and passwords ...”

Heartbleed considered as the worst vulnerability found

TLS Security

- On the Security of the TLS Protocol: A Systematic Analysis (http://eprint.iacr.org/2013/339.pdf)
- TLS Security Where Do We Stand? Kenny Paterson
- SoK: Lessons Learned From SSL/TLS Attacks
- Triple Handshakes and Cookie Cutters: Breaking and Fixing Authentication over TLS
- Revisiting SSL/TLS Implementations: New Bleichenbacher Side Channels and Attacks

Survey of the TLS Vulnerabilities

Survey of the TLS vulnerabilities of the most popular websites

Attacks	Security				
	Insecure		Depends	Secure	Other
Renegotiation attack	N/A	3.7% (−0.2%) support insecure renegotiation	1.2% (±0.0%) support both	90.0% (+0.5%) support secure renegotiation	5.1% (−0.3%) no support
RC4 attacks	1.3% (−0.1%) support only RC4 suites	26.6% (−0.7%) support RC4 suites used with modern browsers	53.2% (−0.7%) support some RC4 suites	20.2% (+1.4%) no support	N/A
BEAST attack (mitigated at client side with modern browsers)	N/A	77.4% (+0.6%) vulnerable	N/A	N/A	N/A
CRIME attack	N/A	7.2% (−0.4%) vulnerable	N/A	N/A	N/A
Heartbleed	N/A	0.3% (−0.1%) vulnerable	N/A	N/A	N/A
ChangeCipherSpec injection attack	N/A	3.3% (−0.4%) vulnerable and exploitable	15.5% (−1.1%) vulnerable, not exploitable	80.1% (+1.3%) not vulnerable	1.0% (+0.1%) unknown
POODLE attack against TLS (Original POODLE against SSL 3.0 is not included)	N/A	10.1% vulnerable and exploitable	N/A	88.4% not vulnerable	1.6% unknown

(Ref. Wikipedia; " ... As of December 2014, Trustworthy Internet Movement estimate the ratio of websites that are vulnerable to TLS attacks. .. ")

TLS and Forward Secrecy

“ .. As of December 2014, 20.0% of TLS-enabled websites are configured to use cipher suites that provide forward secrecy to web browsers ..”

" .. ***Forward secrecy*** is a property of cryptographic systems which ensures that a session key derived from a set of public and private keys will not be compromised if one of the private keys is compromised in the future.

Without forward secrecy, if the server's private key is compromised, not only will all future TLS-encrypted sessions using that server certificate be compromised, but also any past sessions that used it as well (provided of course that these past sessions were intercepted and stored at the time of transmission).

TLS and Forward Secrecy

An implementation of TLS can provide forward secrecy by requiring the use of ephemeral Diffie-Hellman key exchange to establish session keys, and some notable TLS implementations do so exclusively: e.g., Gmail and other Google HTTPS services that use OpenSSL.

However, many clients and servers supporting TLS (including browsers and web servers) are not configured to implement such restrictions.

In practice, unless a web service uses Diffie-Hellman key exchange to implement forward secrecy, all of the encrypted web traffic to and from that service can be decrypted by a third party if it obtains the server's master (private) key; e.g., by means of a court order. ..”

Reference: http://en.wikipedia.org/wiki/Transport_Layer_Security

Transport Layer Security (TLS)

- Advised key exchange methods providing forward secrecy

  TLS_ECDHE_ECDSA_WITH_⋆

  considering security of ECDSA signatures and RSA in the long run.
- Advised ciphers for encrypting the actual data
  - ***Camellia*** and ***AES*** with modes such as GCM or CCM
- Advised hash functions
  - ***SHA256, SHA384***

  (Ref. Enisa “Study on Cryptographic Protocols”, Nov. 2014)
- The Datagram Transport Layer Security (DTLS) protocol provides communications privacy for datagram protocols. The DTLS protocol is based on the stream-oriented Transport Layer Security (TLS) protocol and is intended to provide similar security guarantees.

SSH

- Replacement for insecure protocol for remote access such as telnet
- SSHv2 standardised (RFCs 312,313 and 314)
- most widely used implementation: OpenSSH
- SSH Operations: ***initial key-exchange, server authentication and, confidentiality and integrity*** of messages sent on the channel
- a key-transport method for SSH based on ***1024- bit and 2048-bit RSA*** (RFC 4432)
- ***Ellliptic Curve Cryptography: ECDH and ECMQV*** supported

  (RFC 5656)
- ***SHA-2 for HMAC; Encode-then-Encrypt-and-MAC construction confidentiality***

TCP/IP Layers and Protocols

Application Layer: HTTP, SMTP, DNS, IMAP, DHCP, IMAP, IRC,
Transport Layer: TCP and UDP
Internetwork Layer: IPv4 and IPv6
Network Access Layer: Ethernet

IPSEC

- IPSec: designed to provide security at the IP network layer of the TCP/IP protocol suite.
- The main use of IPSec has been to create virtual private networks (VPNs)
- Two main IPSec protocols called Authentication Header (AH) and Encapsulating Security Payload (ESP) that consider cryptographic algorithms applied for packets.
- Advised
  - ***MAC algorithms*** for future use within IPSec: *HMAC-SHA2-256, HMAC-SHA2-384 ; HMAC-SHA2-512* (RFC4868)
  - ***Symmetric ciphers: AES-CTR*** and ***CAMELLIA-CTR*** in ESP with one of these MAC algorithms
  - ***combined authenticated encryption modes:*** *AES-CCM_⋆, CAMELLIA-CCM_⋆, AES-GCM_⋆, where * either 12 or 16.*

Use of Cryptography in Wireless Communications

- **WPA2(Wifi- Protected Access)** employs the Counter Cipher mode with Message Authentication Code Protocol (CCMP), an encryption scheme that uses AES in CCM mode and offers both message confidentiality and message authentication.
  - No serious attacks are known against the protocol itself.
- Minor weaknesses of the Kasumi block cipher and SNOW 3G known
- UMTS/LTE uses a protocol called ***Authentication and Key Agreement (AKA).***

(Ref. Enisa “Study on Cryptographic Protocols”, Nov. 2014)

Use of Cryptography in Wireless Communications

- **Bluetooth:** in the “pairing” stage, two Bluetooth devices agree on a pair of keys, an initialisation key used for ***mutual authentication via a challenge response protocol based on HMAC-SHA-256***;
  - Starting from Bluetooth 2.1, in order to share link key, ***Elliptic Curve Diffie-Hellman (ECDH)*** implemented
  - Data encryption algorithm: ***stream cipher E0***
  - Message integrity protection: ***a cyclic redundancy code*** implemented

(Ref. Enisa “Study on Cryptographic Protocols”, Nov. 2014)

Use of Cryptography in Wireless Communications

- ***Zigbee*** is a radio communication standard which can be considered to operate mainly at lower power and ranges than Bluetooth.
  - no formal analysis of the protocols
  - key management: ***ECDSA/ECDH*** or by predistribution of symmetric keys
  - main confidentiality algorithms: ***AES in CTR mode***
  - an ***AES based CBC-MAC algorithm*** outputting

    either a 32-bit, 64-bit or 128-bit MAC value
  - authenticated encryption: ***AES in CCM mode***, or a variant of CCM mode called CCM∗
  - ***TLS*** support provided

(Ref. Enisa “Study on Cryptographic Protocols”, Nov. 2014)

A study about improper use of Cryptography in Mobile Applications

- An empirical study shows 10,327 out of 11,748 applications that use cryptographic APIs 88% overall violates rules such as
  - Rule 1: Do not use ECB mode for encryption.
  - Rule 2: Do not use a non-random IV for CBC encryption.
  - Rule 3: Do not use constant encryption keys.
  - + 3 more rules
- Tool CryptoLint, based upon the Androguard Android program analysis framework, developed to identify interactions between cryptographic keys, initialization vectors, and similar cryptographic material and the cryptographic operations

Online Payment

Banks worldwide are starting to authenticate online card transactions using the **'3-D Secure' protocol**, which is branded as **Veried by Visa** and **MasterCard SecureCode**.

3-D Secure™ – Leverages Transport Layer Security (TLS) technology, which is incorporated in most browsers currently in use. Provides confidentiality of information, ensures payment integrity, and authenticates cardholders.

“... 3-D Secure has so far escaped academic scrutiny; yet it might be a textbook example of how not to design an authentication protocol. It ignores good design principles and has signicant vulnerabilities, some of which are already being exploited ...”

Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication (by Steven J. Murdoch and Ross Anderson)

Cryptographic Module Validation Program (CMVP) and FIPS 140-2

- In 1995, the National Institute of Standards and Technology (NIST) established the CMVP that validates cryptographic modules to Federal Information Processing Standards (FIPS)140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards.
- a joint effort between NIST and the Communications Security Establishment Canada (CSEC).
- FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 and supersedes FIPS 140-1
- Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules:

  http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf (Years between 1995-2014)

Hardware Security Modules (HSM)

- A physically and logically protected hardware device that provides a secure set of cryptographic services. It includes the set of hardware, firmware, software, or some combination thereof that implements cryptographic logic, cryptographic processes, or both, including cryptographic algorithms
- "Ref. Page 32 from https://www.pcisecuritystandards.org/documents/PTS_Program_Guide_v1-4_March_2014.pdf "
- **Trusted autorities of X.509 Certificates use HSMs.**
- **For purposes of the requirements of Personal Identification Numbers (PINs) Security, Payment Card Industry (PCI) published HSM requirements**

ISO 13491-1:2007 specifies the requirements for secure cryptographic devices (SCDs) based on the cryptographic processes defined in ISO 9564, ISO 16609 and ISO 11568.

ISO 9564-2:2014 specifies approved algorithms for the encipherment of Personal Identification Numbers (PINs).

Hardware Implementations

- COPACOBANA -Cost-Optimized Parallel Code Breaker
  - FPGA-based machine implementing cryptographic primitivies
  - parallel computation problems which have low communication requirements
  - any symmetric cipher with up to roughly 64 key bits can be attacked
  - its arhitecture well suited for elliptic curve attacks such as the parallel Pollard rho method.
- Other similar hardware EFF's "Deep Crack", TWIRL ,etc.

Lightweight Cryptography

- Aims:
  - achieving high security on (constrained) devices with low computing power
  - securing interconnections between “Things” in The Internet of Things (IoT) such as heart monitoring implants, biochip transponders on farm animals, automobiles with built-in sensors (IPSEC, IPv6 addressing)
  - Primitivies and their cryptanalysis
- Protocols
  - ISO/IEC 29192-2:2012 -- Part 2: Block ciphers (PRESENT, CLEFIA)
  - ISO/IEC 29192-3:2012 - Part 3: Stream ciphers (Enocoro, Trivium)
  - ISO/IEC 29192-4:2013 - Part 4: Mechanisms using asymmetric techniques
  - ISO/IEC CD 29192-5 - Part 5: Hash Functions (Under development)

Some issues in Cloud Computing Security
(Ref. Enisa “Study on Cryptographic Protocols”, Nov. 2014)

- In many cloud applications, basic cryptographic protocols can be deployed to provide security goals.
- In ***Infrastructure as a Service*** (IaaS) model (well-known systems: Amazon’s Elastic Computing Cloud (EC2) and Microsoft’s Azure) one should log into the remote service using ***SSH***
- In all cloud models, web client, browser can be used to access services of a cloud over the web with ***HTTPS*** (HTTP over ***SSL/TLS***)
- In the IaaS model a user selects a given image to install on the virtual machine.
- Needing trust for the image and hypervisor used to share resources between the different virtual machines on the same physical hardware required.
- Direct Anonymous Attestation (DAA) is used to address this issue by utilising ***zero-knowledge protocols*** and some special functionality designed into the TPM chip which sits on most computer motherboard.

Data Security in the Cloud

(Ref. Enisa “Study on Cryptographic Protocols”, Nov. 2014)

Technology	Ready for Deployment	Short Term Research Needed	Longer Term Research Needed
Fully Homomorphic Encryption	×	×	√
Multi-Party Computation	√	√	×
Searchable Encryption	√	√	×
Order Preserving Encryption	×	×	√
Attribute Based Encryption	×	√	×
Delegated Computation	×	×	√
Message Locked Encryption	√	√	×

Table 5.1: Summary of technology readiness of advanced cryptographic mechanisms

Some products based on **MPC** available.

CryptDB considers a sensitive column in the database and then to encrypt it using successively stronger forms of encryption; such as standard encryption, SSE and OPE. The system is efficient, but suffers from inherent leakage of information.
A similar idea to CryptDB is the SEEED system of SAP, which extends the SQL syntax of CryptDB to support more elaborate queries.

Remarks

- Guidelines addressed by researches (*)
  - Many cryptographic and security protocols were not proposed by experts of cryptographic protocols.
  - their design challenging task
  - Necessary to study automated verification tools for their implementation to guarantee correct implementations
- Guidelines for one developing new protocols (*)
  - Ease of formal security analysis and recent studies on cryptanalysis/attacks considered
  - Future protocols should not be any more complex that they need to be (extraneous options used by attacks avoided).
  - Relatively easy to upgrade cryptographic components
  - A secure channel Application Programming Interfaces (APIs) be secure as long as the underlying cryptographic components are secure.

* (Enisa “Study on Cryptographic Protocols”, Nov. 2014):

Remarks

- Important to refer the list of algorithms, the key sizes and other parameters recommended
  - Enisa Algorithms, key size and parameters report 2014
- Using cryptographically secure pseudo random number generators to create keys and other related parameters
- “ ... The trust that users place in secret-key cryptography has been repeatedly and flagrantly violated. . Consider the following recent and ongoing examples: ...”

  “ ... It is easy to blame many of these security problems on a lack of user education, where in this case the users are the software and hardware engineers choosing cryptographic primitives to apply. ..”

  http://competitions.cr.yp.to/disasters.html
- Bad implementations of cryptographic pritimitives and protocols and their improper use in applications should be avoided.
- Important to educate people implementing cryptographic algorithms:

  Educational Tool: Cryptool / Use of Math software such as Sage /

  SEED Project (See Crypto Labs) / Presentation in Turkish