UNIT 2

Why Is Application Security Important?

- New threats emerge every day
- Some hackers are not satisfied with penetrating your network; they seek information that resides in your applications/databases
- Applications are often plagued by poor designs, software bugs, and poor programming practices
- Applications may be a fast and easy entry point into a secure network
- Applications contain and process your most critical (important and sensitive) information
- Programming logic may cause vulnerabilities just as troublesome as difficulties inherent with certain technologies

Four Basic Security Concepts

Poor application security measures can lead to breaches in data:

- Integrity
- Confidentiality
- Availability
- Accountability

Data Integrity

- Protection of information from tampering, forgery, or accidental changes.
  - Defacement of website
    - The White House
    - Amnesty International
  - E-Shoplifting
- The number of vandalized Web sites recorded by defacement archive Alldas.de jumped in 2001 to 22,379, over five times more than the 4,393 defacements logged in 2000.
- January 2004, there were 13,654 known attacks on Linux based WWW systems alone.

Availability

- Ensures that authorized users have access to the application and the data when required.

Confidentiality

- Ensures that applications and data is accessible to only the users intended and authorized to have access.
- Credit Card Theft
  - CD Universe
  - CreditCards.com
  - Guess?
  - Many Others

Accountability Within the Application

- Ensure accuracy of data and guide against unauthorized modifications
- Who did what with your data?
- HIPAA Privacy Regulations: Protected Healthcare Information (PHI)
  - Digital, printed, oral
  - Limited technical guidance
  - Security enables privacy

Applications Must Exist within a Secure Infrastructure

- Harden systems
- Use concept of least-privilege
- Patch management
- Firewalls
- Intrusion detection
- Virus protection
- And Others Tactics…

What is the goal of Application Security?

Prevent the loss, modification, or misuse of application systems "data" or application architecture. Here we are focusing on web-enabled systems

Making an e-commerce application secure is much harder than just adding a password protected login screen!

Securing the Application

- Authentication & Identification
- Authorization & Access Control
- Logging & Auditing Procedures
- Managing User Sessions
- Encryption Routines
- And More…

Access Control

- Identification and authentication (I&A): These determine who can log on to a system.
- Authorization: This determines what an authorized user can do.
- Accountability: This identifies what a user did.

Database Security

- Protect Sensitive Data from
  - Unauthorized disclosure
  - Unauthorized modification
  - Denial of service attacks
- Security Controls
  - Security Policy
  - Access control models
  - Integrity protection
  - Privacy problems
  - Fault tolerance and recovery
  - Auditing and intrusion detection

Protection of Data Confidentiality

- Access control – which data users can access
- Information flow control – what users can do with the accessed data
- Data Mining

Internet Security Today

- What are the main security-related problems on the Internet Today?
  - Hijacked web servers
  - Denial-of-Service Attacks
  - Unsolicited Commercial E-Mail
  - Operator Error, Natural Disasters
  - Eavesdropped electronic mail.
    - (Misdirected email is a problem.)
    - (Email swiped from backup tapes is a problem.)
  - Sniffed credit card numbers.
    - (Credit card numbers stolen from databases is a problem.)
  - Hostile Java & ActiveX applets.

E-Mail Security

- E-Mail Encryption
  - Not widely used because of lack of clear standards
  - IETF has not been able to settle upon a single standard because of in-fighting
  - Three standards are used in corporations
    - TLS
    - S/MIME
    - PGP

E-Mail Security

- E-Mail Encryption
  - TLS only requires a digital certificate for servers
  - S/MIME requires a PKI for digital certificates
  - PGP uses trust among circles of friends: If A trusts B, and B trusts C, A may trust C's list of public keys
    - » Dangerous: Misplaced trust can spread bogus key/name pairs widely

Firewalls

A system of software, hardware or both designed to detect intrusion and prevent unauthorized access to or from a private network

Firewall Techniques

- **Packet Filter** – examine each packet entering and leaving network and accept/reject based on rules
- **Application Level Control** – Performs certain security measures based on a specific application (e.g. file transfer)
- **Keyword** based filtering
- **Destination** (URL) based filtering
    - Certain URLs not permitted (OR)
    - Certain URLs only are permitted

Security Threat: Spyware, Spam, and Cookies

Spyware

Any software that **covertly** gathers information about a user through an Internet connection without the users knowledge

- **Problems**: uses memory resources, uses bandwidth, and can cause system instability
- **Prevention**: Firewalls and Spyware software

Spam

Electronic junk **mail** or junk **newsgroup** postings usually for purpose of advertising for some product and/or service

- **Problems:** nuisance, wastes time deleting, uses storage
- **Prevention:** Spam Blocker software

Cookies

A **message** passed to a browser from a Web server. Used by legitimate programs to store **state** and **user** information

- **Problems**: can be used to track user activities
- **Prevention**: browser settings, firewall

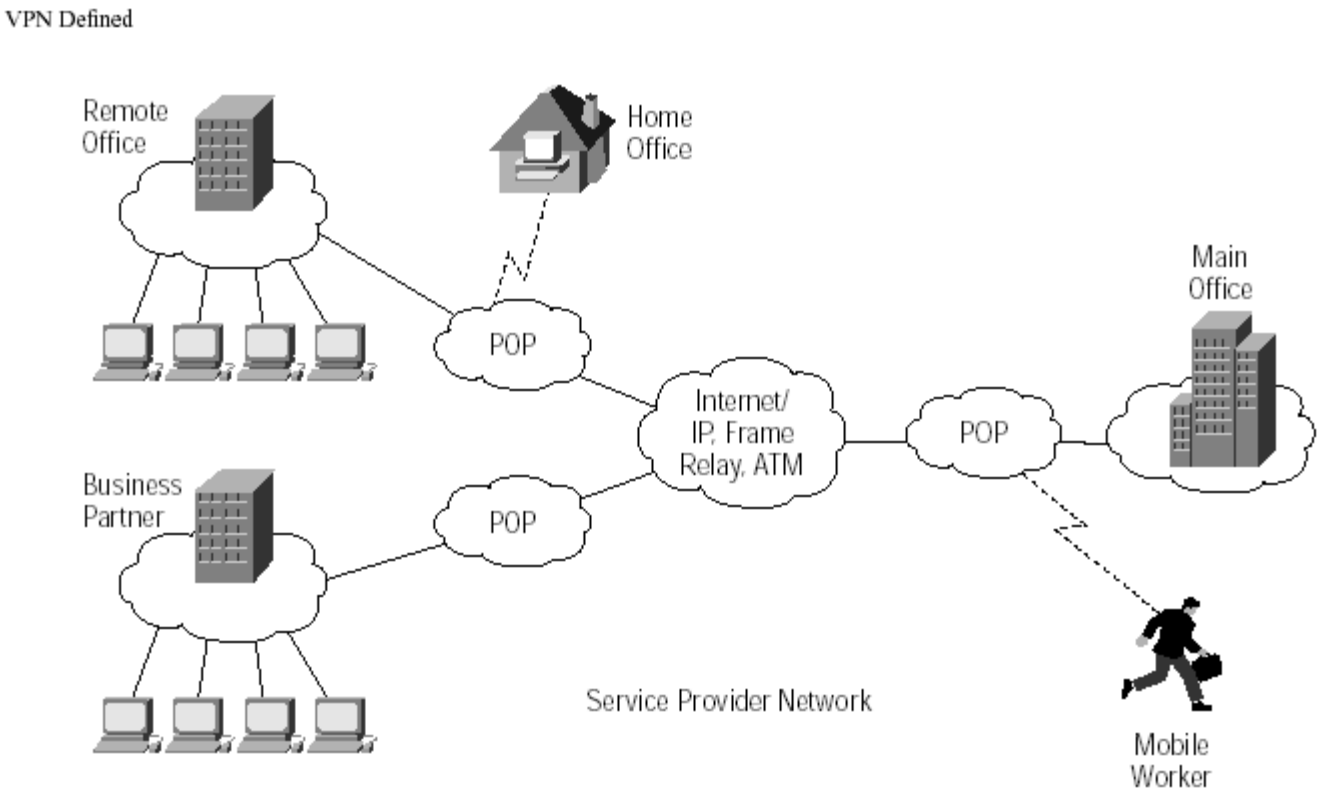
DATA BACKUP

- A **data backup** is the result of copying or archiving files and folders for the purpose of being able to restore them in case of data loss.
- Data loss can be caused by many things ranging from computer viruses to hardware failures to file corruption to fire, flood, or theft (etc). If you are responsible for business data, a loss may involve critical financial, customer, and company data. If the data is on a personal computer, you could lose financial data and other key files, pictures, music, etc that would be hard to replace.

Archival Storage

- In computers, archival storage is storage for data that may not be actively needed but is kept for possible future use or for record-keeping purposes. Archival storage is often provided using the same system as that used for backup storage. Typically, archival and backup storage can be retrieved using a restore process.
- Data archives are often confused with data backups, which are copies of data. Data backups are used to restore data in case it is corrupted or destroyed. In contrast, data archives protect older information that is not needed for everyday operations but may occasionally need to be accessed.

Introduction to VPN



VPN Topology: Advantages and Disadvantages of VPN

- Advantages:
  - Greater scalability
  - Easy to add/remove users
  - Reduced long-distance telecommunications costs
  - Mobility
  - Security

VPN Topology: Advantages and Disadvantages of VPN

- Disadvantages
  - Lack of standards
  - Understanding of security issues
  - Unpredictable Internet traffic
  - Difficult to accommodate products from different vendors

Access Control

- Ensures that all direct accesses to object are authorized
- Protects against accidental and malicious threats by regulating the read, write and execution of data and programs

Intrusion Detection

- Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization)
- ID uses*vulnerability assessment* (sometimes refered to as *scanning*), which is a technology developed to assess the security of a computer system or network.

Intrusion detection functions

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

Threats

Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.

Threats

Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.

Threats

Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Backdoor

- Trapdoor
- Secret entry point
- Useful for debugging tool for programmers

Logic Bomb

- Explodes when certain conditions are met
  - Presence or absence of certain files
  - Particular day of the week
  - Particular user running application

Trojan Horse

- Useful program that contains hidden code that when invoked performs some unwanted or harmful function
- Can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly
  - User may set file permission so everyone has access

Multiple-Threat Malware

- Multipartite virus infects in multiple ways
- Blended attack uses multiple methods
- Ex: Nimda has worm, virus, and mobile code characteristics

Parts of Virus

- Infection mechanism
- Trigger
- Payload

Virus Stages

- Dormant phase
  - Virus is idle
- Propagation phase
  - Virus places an identical copy of itself into other programs or into certain system areas on the disk

Virus Stages

- Triggering phase
  - Virus is activated to perform the function for which it was intended
  - Caused by a variety of system events
- Execution phase
  - Function is performed

Simple Virus

```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
          then goto loop
          else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine triqqer-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

Compression Virus

```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
          {loop:
               file := get-random-executable-file;
          if (first-line-of-file = 01234567) then goto loop;
        (1)    compress file;
        (2)    prepend CV to file;
        }

main:   main-program :=
          {if ask-permission then infect-executable;
        (3)    uncompress rest-of-file;
        (4)    run uncompressed file;}
        }
```

Virus Classification by Target

- Boot sector infector
- File infector
- Macro virus

Virus Classification by Concealment Strategy

- Encrypted virus
  - Random encryption key encrypts remainder of virus
- Stealth virus
  - Hides itself from detection of antivirus software

Virus Classification by Concealment Strategy

- Polymorphic virus
  - Mutates with every infection
- Metamorphic virus
  - Mutates with every infection
  - Rewrites itself completely after every iteration

Macro Viruses

- Platform independent
  - Most infect Microsoft Word documents
- Infect documents, not executable portions of code
- Easily spread
- File system access controls are of limited use in preventing spread

E-Mail Viruses

- Attachment
- Open e-mail
- Uses e-mail software to replicate

Worms

- Use network connections to spread from system to system
- Electronic mail facility
  - A worm mails a copy of itself to other systems

Worms

- Remote execution capability
  - A worm executes a copy of itself on another system
- Remote log-in capability
  - A worm logs on to a remote system as a user and then uses commands to copy itself from one system to the other

Denial-of-service attack

- A type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.

- Many DoS attacks, such as the *Ping of Death* and *Teardrop* attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers.

- Attackers build networks of infected computers, known as 'botnets', by spreading malicious software through emails, websites and social media. Once infected, these machines can be controlled remotely, without their owners' knowledge, and used like an army to launch an attack against any target. Some botnets are millions of machines strong.

Attack Classes

- **TCP Connection Attacks** - *Occupying connections.* These attempt to use up all the available connections to infrastructure devices such as load-balancers, firewalls and application servers. Even devices capable of maintaining state on millions of connections can be taken down by these attacks.
- **Volumetric Attacks** - *Using up bandwidth.* These attempt to consume the bandwidth either within the target network/service, or between the target network/service and the rest of the Internet. These attacks are simply about causing congestion.
- **Fragmentation Attacks** - *Pieces of packets.* These send a flood of TCP or UDP fragments to a victim, overwhelming the victim's ability to re-assemble the streams and severely reducing performance.
- **Application Attacks** - *Targeting applications.* These attempt to overwhelm a specific aspect of an application or service and can be effective even with very few attacking machines generating a low traffic rate (making them difficult to detect and mitigate).

Electronic Commerce Threats

- Secure electronic commerce include protection of three assets in the “commerce chain”.
- These are:
  - Client computers
  - Messages travelling from the client computer to the Web server through the Internet
  - Web/Commerce servers

Client Threats

- Active Content
  - Java applets, Active X controls, JavaScript, and VBScript, which are programs that interpret or execute instructions embedded in downloaded objects from a Web/commerce server
  - Malicious active content can be embedded into seemingly innocuous Web pages
  - **Cookies** remember user names, passwords, and other commonly referenced information

Communication Channel Threats

- Necessity Threats:
  - Also known as delay or denial threats
  - Disrupt normal computer processing
    - Deny processing entirely
    - Slow processing to intolerably slow speeds such that customers get bored not to visit the site anymore.
    - Remove file entirely, or delete information from a transmission or file
    - Divert money from one bank account to another

Server Threats

- The more complex a Web server software becomes, the higher the probability that errors (bugs) exist in the code - security holes through which hackers can access.

- Web servers run at various privilege levels:
  - Highest levels provide greatest access and flexibility to a Web user (from a browser)
  - Lowest levels provide a logical fence around a running program

Database Threats

- A company database systems store data on user, products, and orders for e-commerce
- In addition, a company's valuable and private information could be stored in a company database
- Security in a database is often enforced through defining the user "privileges" which must be enforced
- Some databases are inherently insecure and rely on the Web server to enforce security measures

Other Threats

- Common Gateway Interface (CGI) Threats
  - CGIs are programs that present a security threat if misused
  - CGI programs can reside almost anywhere on a Web server and therefore are often difficult to track down
  - CGI scripts do not run inside a sandbox, unlike JavaScript

Electronic Payment Systems

- Online transaction systems
  - Lack of physical tokens
    - Standard clearing methods won't work
    - Transaction reconciliation must be intermediated
  - Informational tokens
    - Ecommerce enablers
      - First Virtual Holdings, Inc. model
    - Online payment systems (financial electronic data interchange)
      - Secure Electronic Transaction (SET) protocol supported by Visa and MasterCard
    - Digital currency

Electronic Payment Systems

- Digital currency
  - Non-intermediated transactions
  - Anonymity
  - Ecommerce benefits
    - Privacy preserving
    - Minimizes transactions costs
    - Micropayments
- Security issues with digital currency
  - Authenticity (non-counterfeiting)
  - Double spending
  - Non-refutability

Electronic Payment Systems

- Contemporary forms of digital currency
  - Ecash
    - Set up account with ecash issuing bank
      - » Account backed by outside money (credit card or cash)
    - Move credit from account to ecash mint
      - » Public key encryption used to validate coins: third parties can “bite” the coin electronically by asking the issuing bank to verify its encryption
    - Spend ecoin at merchant site that accepts ecash
    - Merchant then deposits ecoin in his account at his participating bank, or keeps it on hand to make change, or spends the ecash at a supplier merchant’s site.
  - Role of encryption

E-CASH

- While many different companies are rushing to offer digital money products, currently e-cash is cash is represented by two models. One is the on-line form of e-cash (introduced by DigiCash) which allows for the completion of all types of internet transactions. The other form is off-line; essentially a digitially encoded card that could be used for many of the same transactions as cash. This off-line version (which also has on-line capabilities) is being tested by Mondex in partnership with various banks.
- The primary function of e-cash is to facilitate transactions on the Internet. Many of these transactions may be small in size and would not be cost efficient through other payment mediums such as credit cards.

Debit cards

- Debit cards are electronic current account cards that offer a safe, convenient alternative to cash and cheques when you wish to make payments. Unlike a credit card, these cards are linked to your current account and you can only spend money that you have; regardless of the type of transaction you make using your card, the funds are always deducted from your current account balance. Debit cards can be used to purchase goods and services in shops, restaurants, garages and supermarkets, as well as online. Debit cards can also be used at Automated Teller Machines (ATMs)

Credit card

- A **credit card** is a payment card issued to users as a system of payment. It allows the cardholder to pay for goods and services based on the holder's promise to pay for them. The issuer of the card creates a revolving account and grants a line of credit to the cardholder, from which the user can borrow money for payment to a merchant or as a cash advance
- Credit cards have higher interest rates (around 19% per year) than most consumer loans or lines of credit. Almost every store allows for payment of goods and services through credit cards. Because of their wide spread acceptance, credit cards are one of the most popular forms of payment for consumer goods and services in the U.S.

What is a digital signature?

- is a type of asymmetric cryptography used to simulate the security properties of a signature in digital, rather than written, form. Digital signature schemes normally give two algorithms, one for signing which involves the user's secret or private key, and one for verifying signatures which involves the user's public key. The output of the signature process is called the "digital signature.“

- is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

How it works

The use of digital signatures usually involves two processes, one performed by the signer and the other by the receiver of the digital signature:

- **Digital signature creation** uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.
- **Digital signature verification** is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

Example

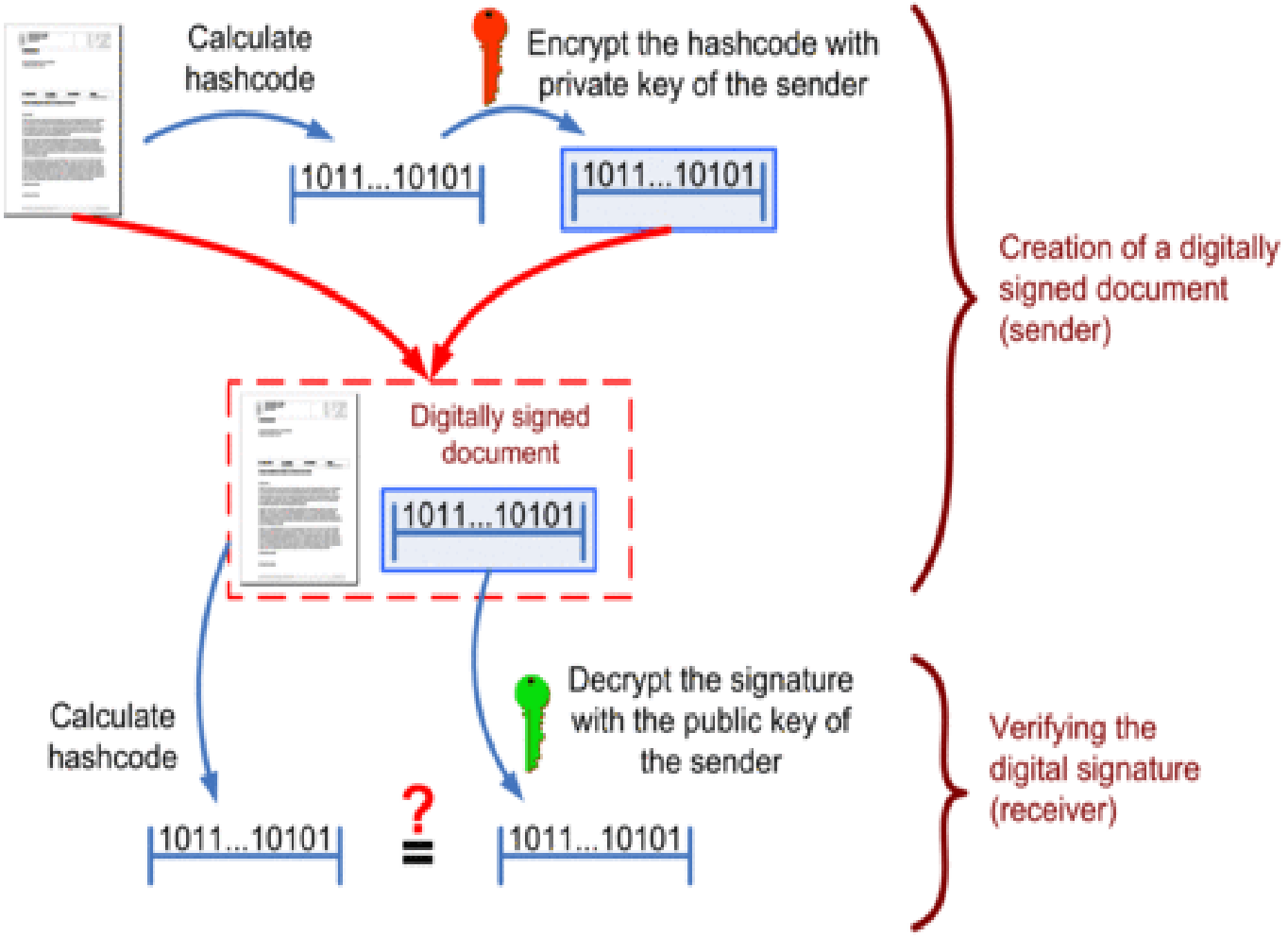
Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

1. You copy-and-paste the contract (it's a short one!) into an e-mail note.
2. Using special software, you obtain a message hash (mathematical summary) of the contract.
3. You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
4. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

1. To make sure it's intact and from you, your lawyer makes a hash of the received message.
2. Your lawyer then uses your public key to decrypt the message hash or summary.
3. If the hashes match, the received message is valid.

Creating and verifying a digital signature



If the calculated hashcode does not match the result of the decrypted signature, either the document was changed after signing, or the signature was not generated with the private key of the alleged sender.

Public Key Cryptography

Rapidly increasing needs for flexible and secure transmission of information require to use new cryptographic methods.

The main disadvantage of the classical cryptography is the need to send a (long) key through a super secure channel before sending the message itself.

In secret-key (symetric key) cryptography both sender and receiver share the same secret key.

In public-key ryptography there are two different keys:
a public encryption key and a secret decryption key (at the receiver side).

Asymmetric-key (public key) encryption

The basic idea:

- A user has two keys: a public key and a private key.
- A message can be encrypted with the public key and decrypted with the private key to provide security.
- A message can be encrypted with the private key and decrypted with the public key to provide signatures.