CAP470: Cloud Computing

Unit-5: Cloud Security and Standards

Contents

- Security in Clouds
- Security Challenges
- Software as a Service Security
- The Open Cloud Consortium
- The Distributed management Task Force
- Standards for application Developers
- Standards for Messaging, Standards for Security
- End user access to cloud computing
- Mobile Internet devices and the cloud

Security in Clouds

“Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use.”

Security Challenges

There are a number of security challenges associated with cloud computing that must be adequately addressed:

1. **Loss of governance**
2. **Responsibility ambiguity**
3. **Authentication and Authorization**
4. **Isolation failure**
5. **Compliance and legal risks**
6. **Handling of security incidents**
7. **Management interface vulnerability**
8. **Application Protection**
9. **Data protection**
10. **Malicious behaviour of insiders**
11. **Business failure of the provider**
12. **Service unavailability**
13. **Vendor lock-in**
14. **Insecure or incomplete data deletion**
15. **Visibility and Audit**

Software-as-a-Service Security

- Cloud computing models of the future will likely combine the use of SaaS (and other XaaS's as appropriate), utility computing, and Web 2.0 collaboration technologies to leverage the Internet to satisfy their customers' needs.
- SaaS will likely remain the dominant cloud service model for the foreseeable future and the area where the most critical need for security practices and oversight will reside.
- With an managed service provider, corporations or end users will need to research vendors' policies on data security before using vendor services to avoid losing or not being able to access their data.

Security Issues

The technology analyst and consulting firm **Gartner** lists **seven security issues** which one should discuss with a cloud-computing vendor:

- **Privileged user access:** Inquire about who has specialized access to data, and about the hiring and management of such administrators.
- **Regulatory compliance:** Make sure that the vendor is willing to undergo external audits and/or security certifications.
- **Data location:** Does the provider allow for any control over the location of data?
- **Data segregation:** Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.
- **Recovery:** Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?
- **Investigative support:** Does the vendor have the ability to investigate any inappropriate or illegal activity?
- **Long-term viability:** What will happen to data if the company goes out of business? How will data be returned, and in what format?

Some Security Practices

SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves.

Security Management and Governance:

- One of the most important actions for a security team is to develop a formal charter for the security organization and program.

- This will foster a shared vision among the team of what security leadership is driving toward and expects, and will also foster "ownership" in the success of the collective team.

- A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies.

Risk Management and Risk Assessment:

- Effective risk management entails identification of technology assets; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities.
- A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or as-needed basis.
- Security risk assessment is critical to helping the information security organization make informed decisions when balancing the dueling priorities of business utility and protection of assets.
- A formal risk assessment process should be created that allocates security resources linked to business continuity.

Security Portfolio Management:

- Security portfolio management is a fundamental component of ensuring efficient and effective operation of any information security program and organization.
- Lack of portfolio and project management discipline can lead to
  - projects never being completed;
  - unsustainable and unrealistic workloads and expectations because projects are not prioritized according to strategy, goals, and resource capacity;
  - and degradation of the system or processes due to the lack of supporting maintenance and sustaining organization planning.
- Portfolio and project management capabilities can be enhanced by developing methodology, tools, and processes to support the expected complexity of projects that include both traditional business practices and cloud computing practices.

Secure Software Development Life Cycle (SecSDLC)

The SecSDLC involves identifying specific threats and the risks, followed by design and implementation of specific controls to counter those threats and assist in managing the risks they pose to the organization and/or its customers. The SDLC consists of six phases, and there are steps unique to the SecSLDC in each of phases:

Phase-1 Investigation: Define project processes and goals, and document them in the program security policy.

Phase-2 Analysis: Analyze existing security policies and programs, analyze current threats and controls, examine legal issues, and perform risk analysis.

Phase-3 Logical design: Develop a security blueprint, plan incident response actions, plan business responses to disaster, and determine the feasibility of continuing and/or outsourcing the project.

Phase-4 Physical design: Select technologies to support the security blueprint, develop a definition of a successful solution, design physical security measures to support technological solutions, and review and approve plans.

Phase-5 Implementation: Buy or develop security solutions. At the end of this phase, present a tested package to management for approval.

Phase-6 Maintenance: Constantly monitor, test, modify, update, and repair to respond to changing threats.

Physical Security of Data Centres:

Data centres must deliver multilevel physical security because mission-critical Internet operations require the highest level of security. The key components of data centre physical security are the following:

- **Physical access control and monitoring:** The data centres should be protected from unauthorised access and for monitoring various security equipment need to be installed.
- **Environmental controls and backup power:** Heat, temperature, air flow, and humidity should all be kept within optimum ranges for the computer equipment housed on-site. Alternate power sources should be available.
- **Policies, processes, and procedures:** As with information security, policies, processes, and procedures are critical elements of successful physical security that can protect the equipment and data housed in the hosting centre.

Standards in Cloud Computing

In Internet circles, everything eventually gets driven by a working group of one sort or another.

- A working group is an assembled, cooperative collaboration of researchers working on new research activities that would be difficult for any one member to develop alone.
- A working group can exist for anywhere between a few months and many years.
- Working groups generally strive to create an informational document a standard, or find some resolution for problems related to a system or network.
- Working groups are sometimes also referred to as task groups or technical advisory groups.

The Open Cloud Consortium (OCC)

The Open Cloud Consortium (OCC)

- Supports the development of standards for cloud computing and frameworks for interoperating between clouds;
- Develops benchmarks for cloud computing; and
- Supports reference implementations for cloud computing, preferably open source reference implementations.
- OCC manages a testing platform and a test-bed for cloud computing called the Open Cloud Test-bed.
- The group also sponsors workshops and other events related to cloud computing.

The OCC is organized into several different working groups.

- **Working Group on Standards and Interoperability for Clouds:** Provide On-Demand Computing Capacity focuses on developing standards for interoperating clouds that provide on-demand computing capacity. One architecture for clouds that was popularized by a series of Google technical reports describes a *storage cloud* providing a distributed file system, a *compute cloud* supporting MapReduce, and a *data cloud* supporting table services. The open source Hadoop system follows this architecture. These types of cloud architectures support the concept of on demand computing capacity.
- **Working Group on Wide Area Clouds and the Impact of Network Protocols on Clouds:** Focus of this working group is on developing technology for wide area clouds, including creation of methodologies and benchmarks to be used for evaluating wide area clouds. This working group is tasked to study the applicability of variants of TCP (Transmission Control Protocol) and the use of other network protocols for clouds.

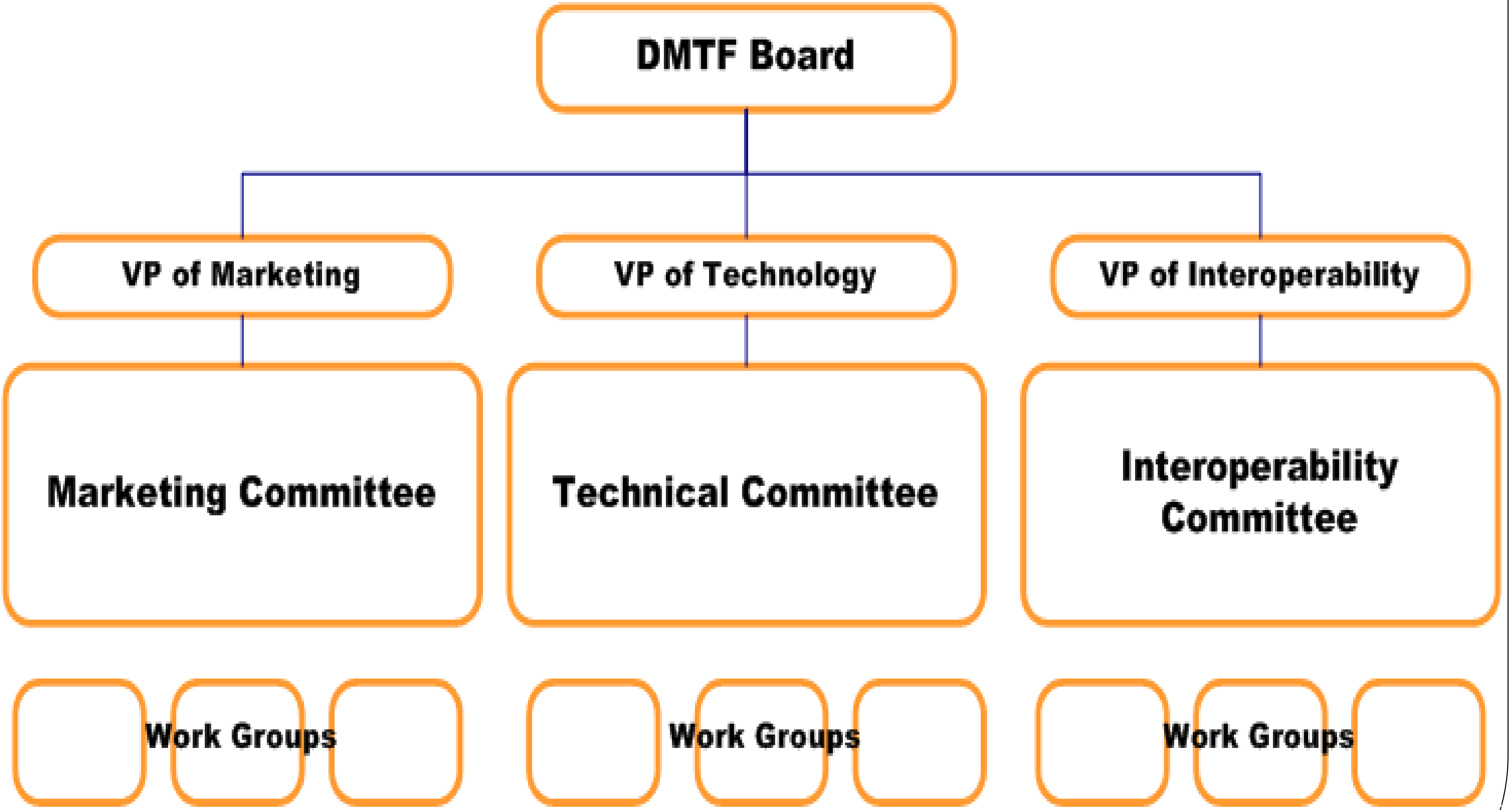
- **The Open Cloud Test-bed Working Group:** It uses Cisco C-Wave and the UIC Teraflow Network for its network connections. C-Wave makes network resources available to researchers to conduct networking and applications research. Experimental and productions networks exist side by side but are physically and operationally separate. Production networks support cutting-edge applications by providing users guaranteed levels of reliability, availability, and performance. At the same time, experimental networks enable the deployment and testing of new networking technologies, providing researchers national-scale testbeds without the limitations typically associated with production networks.

- **Working Group on Information Sharing, Security, and Clouds**: Focus on standards and standards-based architectures for sharing information between clouds. This is especially true for clouds belonging to different organizations and subject to possibly different authorities and policies. This group is also concerned with security architectures for clouds.

Distributed Management Task Force

- With more than 3,500 active participants, the Distributed Management Task Force, Inc. (DMTF) is a not-for-profit, vendor-neutral, collaborative body that is leading the development, adoption, and unification of management standards and initiatives for desktop, enterprise, and Internet environments.
- The Distributed Management Task Force (DMTF) is involved in the development, adoption, and interoperability of management standards and initiatives for enterprise and Internet environments.
- The aim is the exchange of management information in a platform-independent and technology-neutral way, streamlining integration and reducing costs by enabling end-to-end multi-vendor interoperability in management systems.

DMTF Organization



DMTF Board

VP of Marketing

VP of Technology

VP of Interoperability

Marketing Committee

Technical Committee

Interoperability Committee

Work Groups

Work Groups

Work Groups

DMTF Work Groups and Committees

- **DMTF Board:** The DMTF Board is responsible for the overall direction, strategy and activity of the DMTF, including managing DMTF finances, approving technical and marketing initiatives and leading DMTF committee work.
- **Technical Committee:** The Technical Committee develops standards and initiatives for the DMTF and is responsible for coordinating all the technical activities of the DMTF including the Common Information Model (CIM), Web-Based Enterprise Management (WBEM), Management Profiles and Management Initiatives (i.e. SMASH, CDM). The Technical Committee oversees many working groups.
- **Interoperability Committee:** The Interoperability Committee supplements the resources of the DMTF such that multi-vendor implementations of DMTF technologies can be compatible in the industry.
- **Marketing Committee:** The Marketing Committee communicates with the industry, the public, and members about the activities of the organization.

DMTF Standards and Initiatives

The DMTF is leading the development, adoption, and unification of management standards and initiatives for desktop, enterprise and Internet environments. Some of the approved specifications that the DMTF has made public.

- **Common Information Model (CIM):** CIM is a common data model of an implementation-neutral schema for describing overall management information in a network/enterprise environment.
- **Web-Based Enterprise Management (WBEM):** WBEM is a set of management and Internet standard technologies developed to unify the management of enterprise computing environments.
- **Systems Management Architecture for Server Hardware (SMASH) Initiative:** The DMTF SMASH Initiative is a suite of specifications that deliver architectural semantics, industry standard protocols and profiles to unify the systems management of the data centre.

- **Alert Standard Format (ASF):** The ASF specification defines remote control and alerting interfaces that best serve clients' OS-absent environments.
- **System Management BIOS (SMBIOS):** The SMBIOS specification addresses how motherboard and system vendors present management information about their products in a standard format by extending the BIOS interface on Intel architecture systems.
- **Virtualization Management Initiative (VMAN):** The VMAN unleashes the power of virtualization by delivering broadly supported interoperability and portability standards to virtual computing environments.
- **Open Virtualization Format (OVF):** It is a fairly new standard that has emerged within the VMAN Initiative. The OVF simplifies interoperability, security, and virtual machine life-cycle management by describing an open, secure, portable, efficient, and extensible format for the packaging and distribution of one or more virtual appliances.

Standards for Application Developers

The purpose of application development standards is to ensure uniform, consistent, high-quality software solutions.

- **Browsers (Ajax)**
  - Ajax (Asynchronous JavaScript and XML) is a group of interrelated web development techniques used to create interactive web applications or rich Internet applications.
  - Using Ajax, web applications can retrieve data from the server asynchronously, without interfering with the display and behavior of the browser page currently being displayed to the user.
  - The use of Ajax has led to an increase in interactive animation on web pages.

- **Data (XML, JSON)**
  - **XML**
- Extensible Markup Language (XML) is a specification for creating custom markup languages.
- Its purpose is to enable sharing of structured data.
- An XML document has two correctness levels, well formed and valid.
    - A well-formed document conforms to the XML syntax rules.
    - A valid document is well formed and additionally conforms to semantic rules which can be user-defined or exist in an XML schema.
    - XML documents must conform to a variety of rules and naming conventions.
    - XML provides a general, data model-oriented framework for the development of application-specific languages.

- **JavaScript Object Notation (JSON)**
  - JSON is a lightweight computer data interchange format. It is a text-based, human-readable format for representing simple data structures and associative arrays (called objects).
  - The JSON format is often used for transmitting structured data over a network connection in a process called serialization.
  - Its main application is in Ajax web application programming, where it serves as an alternative to the XML format.
  - JSON is based on a subset of the JavaScript programming language.
  - It is considered to be a language-independent data format.
  - Code for parsing and generating JSON data is readily available for a large variety of programming languages.

- **Solution Stacks (LAMP and LAPP)**
  - **LAMP**
    - LAMP is a popular open source solution commonly used to run dynamic web sites and servers.
    - The acronym derives from the fact that it includes **L**inux, **A**pache, **M**ySQL, and **P**HP (or **P**erl or **P**ython).
    - It is considered by many to be the platform of choice for development and deployment of high-performance web applications which require a solid and reliable foundation.
    - When used in combination, they represent a solution stack of technologies that support application servers.

- **Linux, Apache, PostgreSQL, and PHP(or Perl or Python):**
  - The LAPP stack is an open source web platform that can be used to run dynamic web sites and servers.
  - LAPP offers SSL, PHP, Python, and Perl support for Apache2 and PostgreSQL.
  - There is an administration front-end for PostgreSQL as well as web-based administration modules for configuring Apache2 and PHP.
  - LAPP stack considered as a more secure out-of-the-box solution than the LAMP stack.

Standards for Messaging

A *message* is a unit of information that is moved from one place to another.

- **Simple Message Transfer Protocol (SMTP)**
  - SMTP is usually used for either sending a message from a workstation to a mail server or for communications between mail servers.
  - SMTP was designed so that sender and recipient information could be transmitted with the message.
  - SMTP is a two-way protocol that usually operates using TCP (Transmission Control Protocol) port 25.

- **Post Office Protocol (POP):**
  - POP is a lightweight protocol whose single purpose is to download messages from a server.
  - This allows a server to store messages until a client connects and requests them.
  - Once the client connects, POP servers begin to download the messages and subsequently delete them from the server (a default setting) in order to make room for more messages.
  - Users respond to a message that was downloaded using SMTP.
  - The POP protocol is defined by RFC 1939 and usually functions on TCP port 110.
- **Internet Messaging Access Protocol (IMAP):**
  - IMAP allows messages to be kept on the server but viewed and manipulated (usually via a browser) as though they were stored locally.
  - IMAP is a part of the RFC 2060 specification, and functions over TCP port 143.

- **Syndication (Atom, Atom Publishing Protocol, and RSS)**

Content syndication provides citizens convenient access to new content and headlines from government via RSS (Really Simple Syndication) and other online syndication standards.

Benefits:

- Ability to scan headlines from many sources, all in one place, through a newsreader.
- Time-saving awareness of new content from government, if the RSS feed or feeds are designed properly.
- Ability to monitor new content from across the council, as well as display feeds on their own web site.
- Awareness of new content position councilors as guides to government for citizens.
- Ability to aggregate new content or headlines from across multiple
- office locations and agencies.

- **Limitations:**
  - Dissemination via syndication is a new concept to governments just getting used to the idea of remote online public access to information.
  - Governments need to accept that while they control the content of the feed, the actual display of the headlines and content will vary.
  - Popular RSS feeds can use significant amounts of bandwidth.
  - Automated syndication requires use of a content management system.
  - Most viable content management systems have integrated RSS functions, but the sophistication, ease of use, and documentation of these tools vary.

- **RSS**
  - RSS is a family of web feed formats used to publish frequently updated works - such as blog entries, news headlines, audio, and video in a standardized format.
  - An RSS document includes full or summarized text, plus metadata such as publishing dates and authorship.
  - RSS feeds can be read using software called a reader that can be web-based, desktop-based, a mobile device, or any computerized Internet-connected device.
  - A standardized XML file format allows the information to be published once and viewed by many different programs.
  - The user subscribes to a feed by entering the feed's URI into the reader or by clicking an RSS icon in a browser that initiates the subscription process.
  - The RSS reader checks the user's subscribed feeds regularly for new work, downloads any updates that it finds, and provides a user interface to monitor and read the feeds.

- **Atom and Atom Publishing Protocol (APP)**
  - The name Atom applies to a pair of related standards.
  - The Atom Syndication Format is an XML language used for web feeds, while the Atom Publishing Protocol (AtomPub or APP) is a simple HTTP-based protocol for creating and updating web resources, sometimes known as web feeds.
  - Web feeds allow software programs to check for updates published on a web site.
  - To provide a web feed, a site owner may use specialized software (such as a content management system) that publishes a list (or "feed") of recent articles or content in a standardized, machine-readable format.
  - The feed can then be downloaded by web sites that syndicate content from the feed, or by feed reader programs that allow Internet users to subscribe to feeds and view their content.
  - A feed contains entries, which may be headlines, full-text articles, excerpts, summaries, and/or links to content on a web site, along with various metadata.
  - The Atom format was developed as an alternative to RSS.

- **Web Services (REST)**
  - REpresentational State Transfer (REST) is a style of software architecture for distributed hypermedia systems such as the World Wide Web.
  - REST refers to a collection of network architecture principles which outline how resources are defined and addressed.
  - An important concept in REST is the existence of resources, each of which is referenced with a global identifier (e.g., a URI in HTTP).
  - REST provides improved response time and reduced server load due to its support for the caching of representations.
  - REST improves server scalability by reducing the need to maintain session state.
  - REST requires less client-side software to be written than other approaches, because a single browser can access any application and any resource.

- **SOAP**
  - SOAP, originally defined as Simple Object Access Protocol, is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks.
  - SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework on which web services can be built.
  - The SOAP architecture consists of several layers of specifications for message format, message exchange patterns (MEPs), underlying transport protocol bindings, message processing models, and protocol extensibility.
  - SOAP is platform-independent, language-independent, and it is simple and extensible.

- **Communications (HTTP, SIMPLE, and XMPP)**
- **Hypertext Transfer Protocol (HTTP)**
  - HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems.
  - Its use for retrieving linked resources led to the establishment of the World Wide Web.
  - HTTP is a request/response standard between a client and a server. A client is the end-user, the server is the web site.

- **SIMPLE**
  - Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) is an instant messaging (IM) and presence protocol suite based on the Session Initiation Protocol (SIP).
  - The core protocol methods provide SIP extensions for subscriptions, notifications, and publications. The methods used, subscribe and notify.
  - **Subscribe** allows a user to subscribe to an event on a server.
  - **Notify** is the method used whenever the event arises and the server responds back to the subscriber.
- **XMPP**
  - Extensible Messaging and Presence Protocol (XMPP) is an XML-based protocol used for near-real-time, extensible instant messaging and presence information.
  - XMPP remains the core protocol of the Jabber Instant Messaging and Presence technology.
  - Jabber provides a carrier-grade, best-inclass presence and messaging platform.

Standards for Security

- Security standards define the processes, procedures, and practices necessary for implementing a security program.
- These standards also apply to cloud related IT activities and include specific steps that should be taken to ensure a secure environment is maintained that provides privacy and security of confidential information in a cloud environment.
- Security standards are based on a set of key principles intended to protect this type of trusted environment.
- **SAML, OAuth, OpenID, SSL/TLS**

- **Security Assertion Markup Language (SAML)**
  - SAML is an XML-based standard for communicating authentication, authorization, and attribute information among online partners.
  - It allows businesses to securely send assertions between partner organizations regarding the identity and entitlements of a principal.
  - SAML protocol refers to what is transmitted, not how it is transmitted.
- **Open Authentication (OAuth)**
  - OAuth is an open protocol to allow secure API authorization in a simple, standardized method for various types of web applications.
  - OAuth is a method for publishing and interacting with protected data.
  - The Core deals with fundamental aspects of the protocol, namely, to establish a mechanism for exchanging a user name and password for a token with defined rights and to provide tools to protect the token.
  - With Oauth, sites use tokens coupled with shared secrets to access resources.
  - Secrets, just like passwords, must be protected.

- **OpenID**
  - OpenID is an open, decentralized standard for user authentication and access control that allows users to log onto many services using the same digital identity.
  - It is a single-sign-on (SSO) method of access control.
  - As such, it replaces the common log-in process (i.e., a log-in name and a password) by allowing users to log in once and gain access to resources across participating systems.
- **SSL/TLS**
  - Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographically secure protocols designed to provide security and data integrity for communications over TCP/IP.
  - TLS and SSL encrypt the segments of network connections at the transport layer.
  - Several versions of the protocols are in general use in web browsers, email, instant messaging, and voice-over-IP.

End user access to cloud computing

- Users access cloud computing using networked client devices, such as desktop computers, laptops, tablets and smartphones. Some of these devices - *cloud clients* - rely on cloud computing for all or a majority of their applications so as to be essentially useless without it. Examples are thin clients and the browser-based Chromebook.
- Many cloud applications do not require specific software on the client and instead use a web browser to interact with the cloud application.
- With Ajax and HTML5 these Web user interfaces can achieve a similar or even better look and feel as native applications. Some cloud applications, however, support specific client software dedicated to these applications (e.g., virtual desktop clients and most email clients).
- Some legacy applications (line of business applications that until now have been prevalent in thin client Windows computing) are delivered via a screen-sharing technology.

- YouTube, an online video repository, has an amazing hold on the global audience.
- Collaboration suites such as Zimbra both enhance mobility and allow you to maintain a virtual office in the cloud.
- Social networking with Facebook has become very popular, especially in academic settings.
- Zoho is a SaaS vendor to watch. Backed by Google, Zoho offers something for everyone.
- For presentations and online sharing, Dimdim is a good choice.

Mobile Internet Devices

- A **mobile Internet device** (MID) is a multimedia-capable **mobile device** providing **wireless Internet** access.
- They are designed to provide entertainment, information and location-based services for personal or business use. They allow 2-way communication and real-time sharing.