Course: Information Security Management in e-Governance

Day 1

Session 4: Securing Business Applications

Agenda

- Introduction to categories and definition of business applications
- Information security risks in application softwares
- Information security solutions and standards for securing business applications

Defining Application Software

Computer Software (SW), consisting of programs, enables a computer to perform specific tasks, as opposed to its physical components (hardware or HW) which can only do the tasks they are mechanically designed for.

There are three major categories of computer software:

- **System Software** helps run the computer hardware and computer system (e.g. operating systems, device drivers, diagnostic tools, servers, windowing systems, and utilities).
- **Programming Software** provides tools to assist a programmer in writing computer programs (codes) using different programming languages in a more convenient way (e.g. code editors, compilers, interpreters, linkers, debuggers).
- **Application Software** allows end users to perform/accomplish one or more specific business operations/tasks.

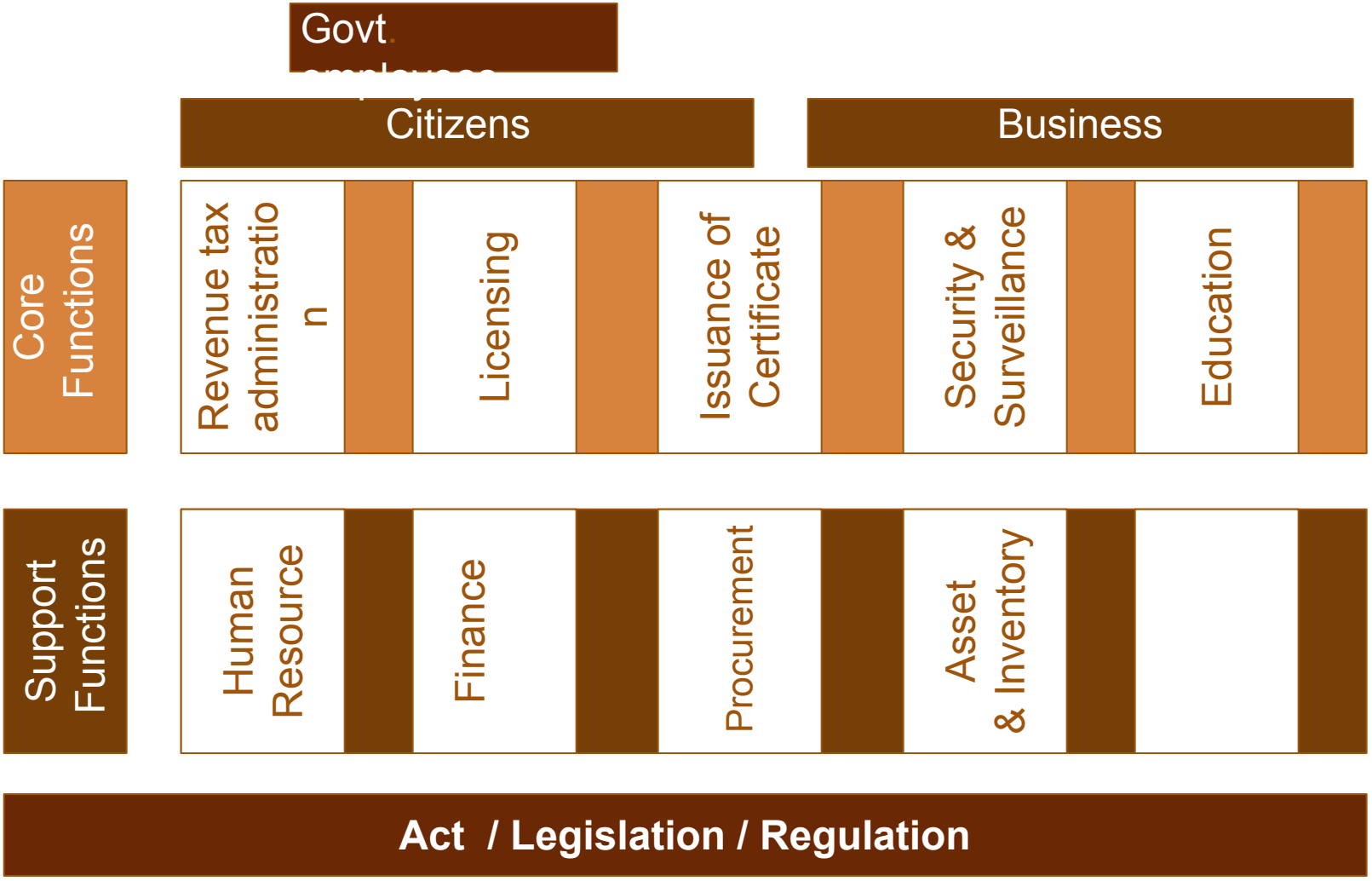
Defining Application Software

Categories of Application Software (ASW):

- **Commercial-off-the-Shelf (COTS) Software**
  - is a term for ready-made application software, available for sale, lease, or license to end users.
  - COTS software is available for most of the support functions of the government and for some of the core functions of the government (e.g. HR, Finance, Supply chain, Tax and Revenue management..)

- **Custom Developed Software (CDSW)** I
  - “in-house developed” (or “bespoke” or “tailored”) software designed to meet the specific needs of end users/organizations.
  - Most of the government entities in India are currently adopting custom developed software approach..

Illustrative business functions in government sector…..



Applications software supporting government business functions..

Support functions application (example)

- **HRMS** : Payroll , Work Time, Administration, HR management Information system, Recruiting, Performance record, Employee Self-Service etc.
- Others such as Financial Management , asset management etc

Core functions application (example)

- **Land registration :** Land registration , issuance of certificates etc.
- Other applications as e-police , e-health , Revenues , tax etc.

- Applications forms the backbone of the core and support functions of governments
- Most of the business functions of governments revolve around applications
- Application performance can be unique based on individual application requirements and user expectations.

Information Security Risks surrounding business applications

Risks surrounding business applications

- **Unauthorized access:** It is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner
- **Unauthorized transactions:** Unauthorized transactions are transactions without proper authorization
- **Data Manipulation:** A way in which data can be manipulated and changed
- **Data Loss**: Data loss refers to the unforeseen loss of data or information
- **Denial of Services**: A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users
- **Data theft:** When information is illegally copied or taken from a business or other individual

Security Compromise : Outcome

- Theft and fraud
- Loss of confidentiality
- Loss of privacy
- Loss of integrity
- Loss of availability
- Loss of Revenue
- Goodwill loss
- And so many……..

The most common Business Application security issues

- Inadequate IT Security and IT involvement during definition, design testing & review
- Inadequate development team knowledge - application security threats & secure application development principles
- Inadequate security controls throughout the SLDC (e.g. Security Considerations during Business Impact and Threat Assessments, Problem and Change Management, Testing)
- Inadequate security testing
- Bespoke and rapid development of applications
- Inadequate independent and qualified security assessments
- Unqualified assessors undertaking security reviews

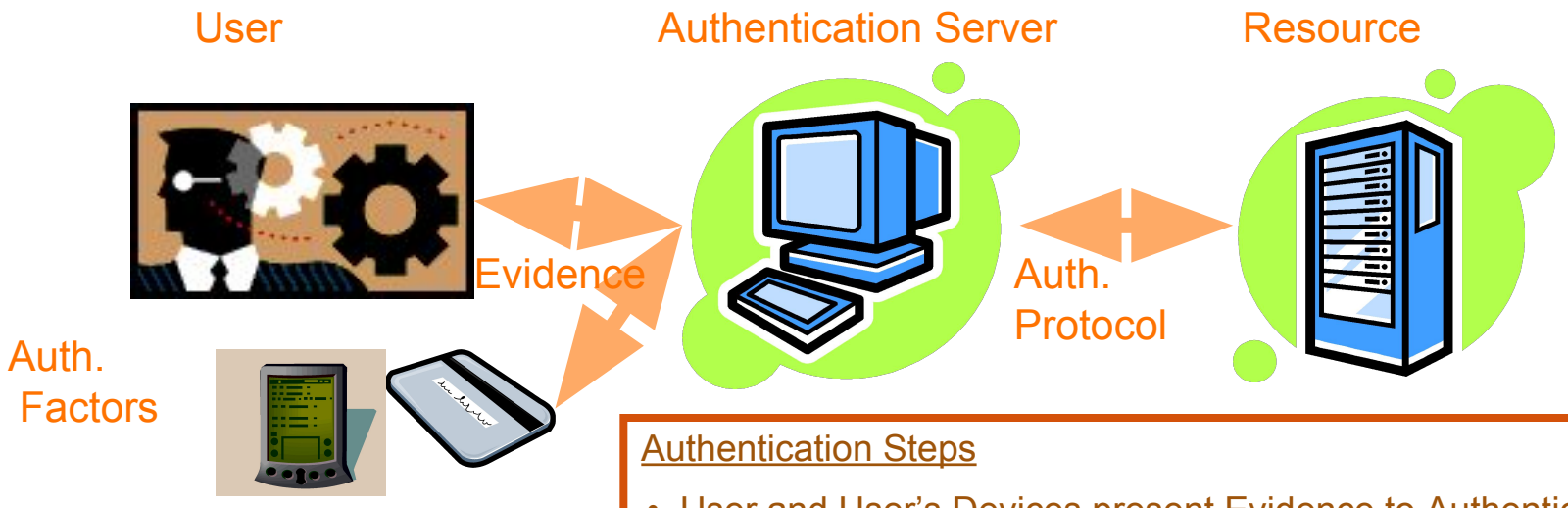
Approach for securing business applications

Key Focus areas in Application Security

- Authentication - How do I know who this is ?
    - Ability to Validate
    - Proving Identity
- Authorization - How do I know what he/she can access?".
    - Allowing to Transact
- Accounting - How to I check what is happening in the system ?
    - Audit Trails
- Users Management - How do I manage this identity and what it can access over its lifetime?
    - Management
    - Profiling

Authentication

- Authentication services facilitate the process of determining who a user is
- An organisation may support multiple authentication schemes and mechanisms
- Authentication systems must be able to reliably verify the identity of the individual or organizational customer
- Authentication can be single factor or two factor or three factor authentication



Authentication Steps

- User and User's Devices present Evidence to Authentication Server demonstrating possession of Authentication Factors
- Authentication Server conveys Evidence to Resource in Authentication Protocol

Variations on the Model

- **Local authentication:** User authenticates directly to resource, without authentication server
    - e.g.: Log into PC; Unlock smart card
- **Authentication server:** User authenticates once to authentication server, which relays ticket or authentication assertion to resource
    - e.g.: Kerberos; Identity providers
- **Validation server:** Resource relies on separate validation server for part or all of authentication decision
    - e.g.: Credential federation
- **Contextual factors:** Where & when did the protocol originate?

Describing an Authentication Mechanism

- An authentication mechanism is a process involving:
  - Selected authentication factors
  - Particular evidence about those factors; and a
  - Specific protocol for conveying the evidence
- *Simple authentication mechanism* has one resource, one authentication decision

Authentication Factors

Something you know:

• Password	Password
• Knowledge-based authentication	Answer

Something you have:

• One-time password token	One-time password
• Smart card / USB token	Signature

Something you are / can do:

- Biometrics — Fingerprint

Strong Authentication

- A system may recognise one or more of three factors to be used for authenticating users:
  - 'Something you know', such as a password, PIN or an out of wallet response,
  - 'Something you have', such as a mobile phone, credit card or hardware security token
  - or 'Something you are', such as a fingerprint, a retinal scan, or other biometric.
- Strong authentication will entail using more than one of these authentication factors at any one time.

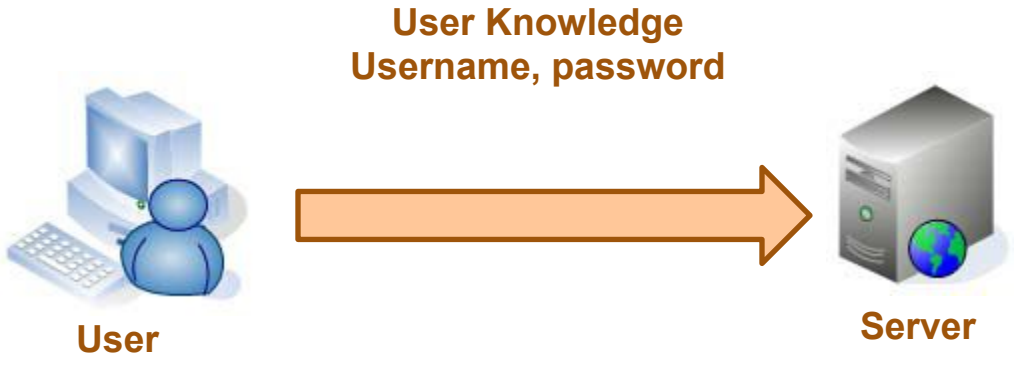
Authentication factors

- User Knowledge
  - Username/Password
  - pass phrase
  - PIN Code
- User Attribute
  - Fingerprint
  - Iris Scan
  - Hand Geometry
  - Voice Print
  - Facial Image
  - DNA sequence
  - Signature

- User Possession
  - Security Token
  - Security Card
  - Certificate

Single Factor Authentication (SFA)

- SFA is the traditional security process that requires a user name and password before granting access to the user.
- SFA security relies on the diligence of the user, who should take additional precautions -- for example, creating a strong password and ensuring that no one can access it.
- Single factor authentication needs an enhanced security environment for users to authenticate and transact on web
- It also needs a mechanism to have a centralized repository of User profiles and credentials



Single Factor Authentication

User Id Rules – Best Practices for User ID creations - Illustrative

- Definition and implementation of policy and procedures for creation and management of user id's
- There should be a one-to-one relationship between user Ids and individuals.
- Access to computing resources (e.g. files, applications, and databases) via shared User Ids should be strictly prohibited
- Deactivation of user accounts, which are inactive for long durations (e.g. more than 60 days)
- User Ids with special system privileges should be controlled and restricted to a limited number of authorised personnel
- Administrators should logon as themselves, using a normal User Id when performing regular work duties rather than logging in as the Supervisor/Administrator
- Logging in as the Supervisor/Administrator should be limited to administrative activities only
- "Guest" accounts or features (where applicable) should be disabled

Strong password

- A strong password is one that is designed to be hard for a person or program to discover.
- Because the purpose of a password is to ensure that only authorized users can access resources, a password that is easy to guess is a security risk.
- Essential components of a strong password include sufficient length and a mix of character types.
- A typical weak password is short and consists solely of letters in a single case.

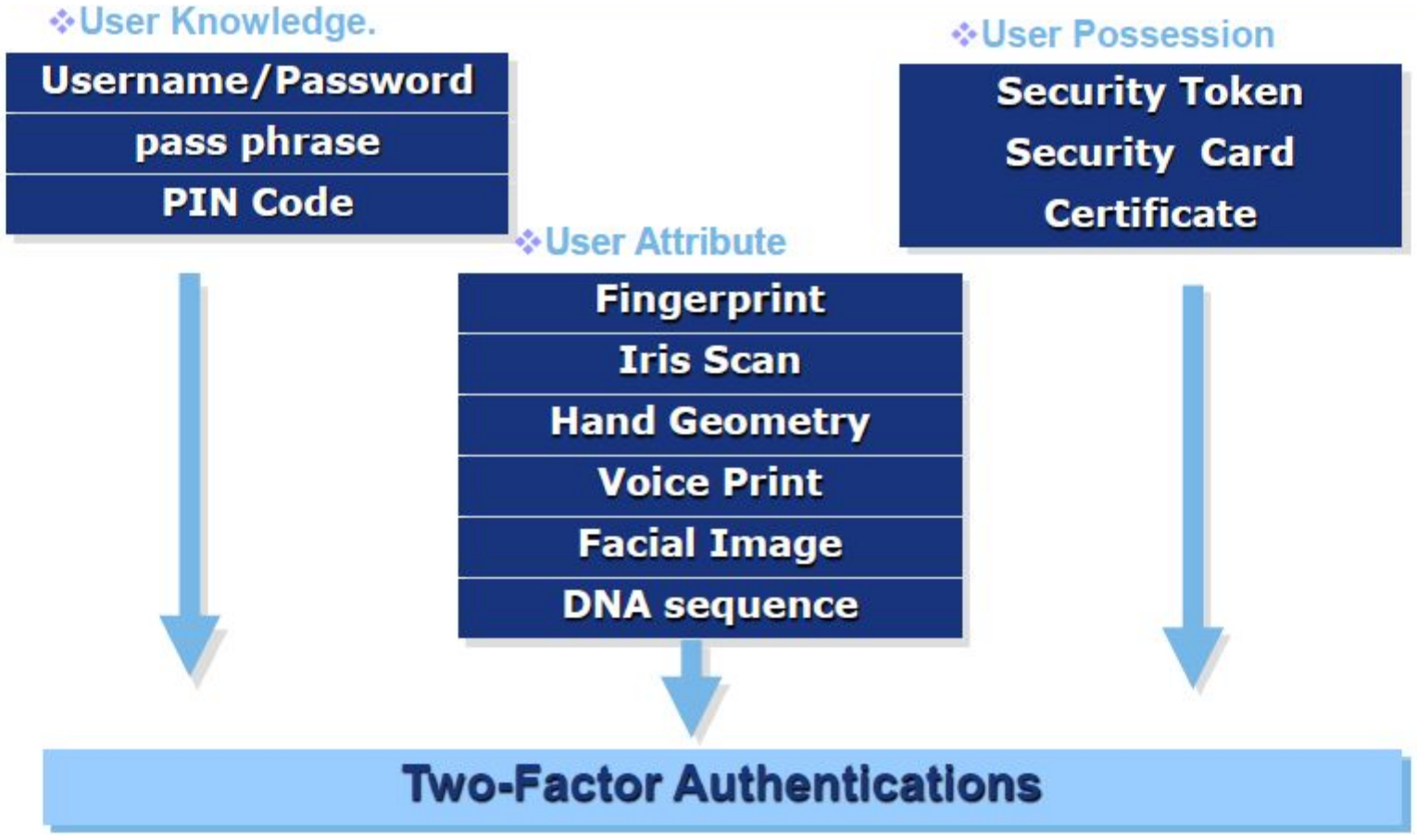
Password Management – Illustrative Best Practices

- The minimum length of passwords should be set as 8 characters and alphanumeric
- Password expiration period of 1 or two month should be set to force users to change their passwords at regular intervals
- Passwords should never be displayed, stored or transmitted in clear text
- The system should force the user to change the password (issued by the Systems Administrator) at the time of the initial logon
- User Ids should be disabled after incorrect passwords have been entered for 3 consecutive times.
- Default passwords, shipped with software upon installation of the software or receipt of a system with pre-loaded software, should be immediately changed.
- The practice of "recycling" or reusing the same password when prompted for a change should be prevented, where possible.
- System files holding authentication data or passwords should be protected from unauthorised access

Challenges with Single factor authentication / passwords

- When they are memorable, they are weak
- When they are strong, they are unmanageable
- People almost always either pick weak passwords *or* they record their passwords someplace handy (perhaps protected by a single password)

Two factor authentication



What is 2-3 Factor Authentication

- Is a combination of Something you know (Password), Something you have (Smart Card / tokens) and/or Something you are (Biometric)
- Authentication using two or three independent methods – typically something you have (device) and something you know (password)
- A reusable password plus a physical device greatly increases the security around authentication
- Two-Factor authentication is being more widely embraced by the banking and financial services industries
- Most common example: ATMs require that you have a reusable password (PIN) and a physical card in order to access bank account
- Examples: Digital Certificates, Smart Cards, RSA Tokens. Biometrics…

Digital Certificates

- Digital Client certificates are solution for enabling the enhanced user identification and access controls needed to protect sensitive online information
- Used to authenticate an individual & issued by trusted third parties known as Certificate Authorities (CAs)
- It is given at various security levels. Higher the security level, the CA verifies the authenticity of the certificate seeker more.
- Digital certificates can also be stored and transported on smart cards or USB tokens for use when traveling
- Digital Certificates can be issued by any one as long as there are people willing to believe them

Classes of Public Key Certificates

- **Class 0 Certificate:** This certificate shall be issued only for demonstration/ test purposes.
- **Class 1 Certificate:** Will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database.
- **Class 2 Certificate:** Will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.
- **Class 3 Certificate:** High assurance certificates and primarily intended for e-commerce applications

List of Certificate Issuing Authorities:

- Safescrypt – Sify communications Ltd
- IDRBT Certifying Authority – IDRBT
- National Informatics Centre
- Tata Consultancy Services
- mtnlTrustLine – MTNL
- Code Solutions Certifying Authority - Code Solutions
- e-Mudhra - 3i Infotech Consumer Services

Retrieved from http://cca.gov.in on 12/06/2010

Few areas where Digital certificates are prominently used in governments

- MCA-21 : Requires a Class 2 or Class 3 individual signature
- e - procurements applications
- e-mudhra
- E- filing of patents…

Security token & Smart Cards

Security Token

- One form of 'something you have' is the smart card and USB tokens
- If the security token is a software token, it is usually associated with a particular workstation
- Security tokens use two-factor authentication using a password and a device (or an appropriate hardware identifier)
- Security token is usually a hardware device such as a Smart Card

Smart Cards

- Tamperproof, electronic storage of PKI keys.
- Can be uploaded or generated on the card
- Cards do not release the keys but rather perform the signing operation on the card
- Card can run applets/applications which are written in Java and other common languages.

One-time password (OTP)

- A One-time password has a limited duration validity on a single use
- These devices have an LCD screen which displays a pseudo-random number consisting of 6 or more alphanumeric characters
- Generated using a counter-based token or a clock-based token
- Counter-based token is an active token that generates a one-time password based on a counter in the server and the secret key of the user
- Clock-based token is an active token that generates one-time passwords based on the server clock

Something you are: biometrics

Usage of “something you are”

- Biometric authentication involves unique physical or behavioral characteristics of individuals
- Fingerprint, Facial, Retinal, Iris, Voice, Hand Geometry
- Prevents unauthorized access by requiring cardholder to be present
- Can be combined with “something you know” = PIN and “something you have” = smart card.

Few methods / protocols for authentication

LDAP

- The Lightweight Directory Access Protocol (or LDAP) provides networked access to a hierarchical database of authentication information.
- LDAP is appropriate for any kind of directory-like information, where fast lookups and less-frequent updates are the norm making it perfect for use in authenticating an organisation's users.

Kerberos

- Kerberos is a network authentication protocol that will allow individuals communicating over an insecure network to prove their identity to one another in a secure manner.
- Kerberos is a client-server model that provides mutual authentication, thereby allowing both the user and the server verify each other's identity

Native Authentication

- Native authentication schemes are authentication mechanisms built into devices and/or some applications that often utilise proprietary authentication protocols and non standardised authentication information stores.

Single Sign On - SSO

- Single sign-on (e-SSO) is a property of authentication for multiple, related, but independent software systems.
- With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them.
- The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.
- The user's credentials are stored in a very secure cryptographically locked store and that the users themselves no longer know the applications credentials, it's possible to 'release' (logon with) certain credentials based on a defined 'authentication grade'.
- Two factor authentication systems such as smart cards or biometrics can be linked to different authentication grades.

SSO - Advantages

- Reduced operational cost
- Reduced time to access data
- Improved user experience, no password lists to carry
- Advanced security to systems
- Strong authentication
  - One Time Password devices
  - Smartcards
- Centralized management of users, roles
- Fine grained auditing

Authorisation

- Once we know (reasonably) *who it is,* we need to decide *what they can access, and how.*
- Authorisation facilitate the process of determining what a user is entitled to access
- **Authorization** is the function of specifying access rights to resources, which is related to information security and computer security in general and to access control in particular.
- When a user tries to access a resource, the access control process checks that the user has been authorized to use that resource
- Users should only be authorized to access whatever they need to do their jobs !!!

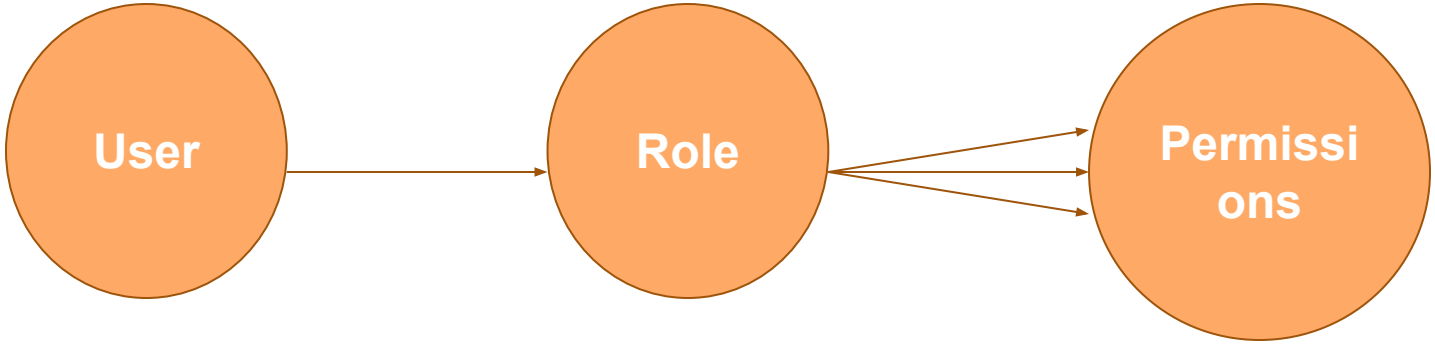
Authorisation

Role Based Access Control

- Authorise users of systems based on predefined privileges that are associated with a job function.
- Hence the access users would gain to systems should be restricted to their role within the organisation, and when the user changes roles, the user's access to systems changes as well.
- Access to systems within the organisation should be based on roles wherever possible.
- For e.g. depending upon the need the final approval of an land allotment application should be restricted to some members of the approving committee.

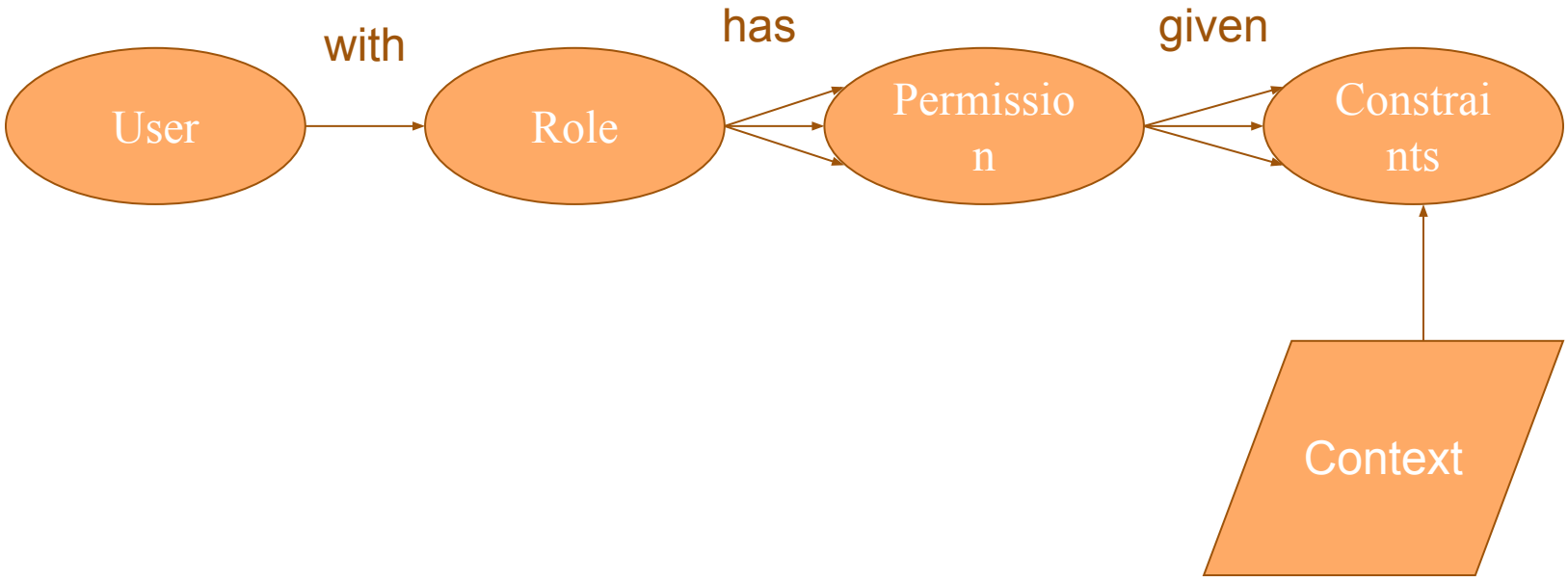
Role-Based Access Control

- During operation, the system uses the access control rules to decide whether access requests from (authenticated) users shall be granted or rejected.
- Resources include individual files' or items' data, computer programs, computer devices and functionality provided by computer applications.



Context-Based Access Control

- Trusted users that have been authenticated are often authorized to unrestricted access to resources.
- "Partially trusted" will often have restricted authorization in order to protect resources against improper access and usage



Authorisation

Context / Rule Based Access Control

- Access to systems within the organisation also support rules / context wherever needed.
- Context / Rule based access control seeks to authorise users of systems based on predefined rules that are associated with an identity or set of identities
- Hence the access users would gain to systems will be restricted to rules set by the organisation, and when the rules change, the user's access to systems changes as well.
- For e.g. in case of land allotment application, once the application is processed , a rule can be set which only allows the managing director to change the allotted value etc.

Some of the best practices for authorization

- Users' access rights should be reviewed at an interval of 3 months. However, authorisations for special privileged access rights should be reviewed at an interval of 1 months.

- The Systems Security Administrator should review user access rights when changes to a user's normal duties are required, for example, as a result of resignation, termination, transfer or promotion.

Solutions/Tools for Authorization implementation?

Audit and Audit trails

- **Audit** – the process of reviewing activities that enables the reconstruction and examination of events to determine if proper procedures have been followed.
- System logs of “who was on what system when” depend on Authentication credentials of the user
- The Audit element provides a control mechanism that is used to
  - ➢ determine whether policy objectives are being met,
  - ➢ to determine and verify privilege settings,
  - ➢ to determine whether users have accounts on the appropriate systems,
  - ➢ to create audit trails of activity, as well as
  - ➢ to determine whether segregation of duties is being enforced.
- Audit records typically result from activities such as transactions or communications by individual people, systems, accounts or other entities.

Audit trails - Need

Individual Accountability

- An individual's actions are tracked in an audit trail allowing users to be personally accountable for their actions.
- This deters the users from circumventing security policies. Even if they do, they can be held accountable.

Reconstructing Events

- Audit trails can also be used to reconstruct events after a problem has occurred.
- The amount of damage that occurred with an incident can be assessed by reviewing audit trails of system activity to pinpoint how, when, and why the incident occurred.

Audit trails and similar evidence is needed for

- Monitoring and reviewing any application access related breaches;
- Use of evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings e.g. under Copyrights Act, Information Technology Act

Audit trails - Need

- **Problem Monitoring**
  - Used as on-line tools to help monitor problems as they occur.
  - Real time monitoring helps in detection of problems like disk failures, over utilization of system resources or network outages.
- **Intrusion Detection**
  - Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access.
  - Audit trails can help in intrusion detection if they record appropriate events.
  - Determining what events to audit so that audit trails can be used in an effective manner to aid intrusion detection is one of the present research issues being looked into by the research community.

Audit trail – Need

Reporting

- The Reporting element enables the organisation to draw a variety of reports relating to the use of its identities.
- In particular, reports on audit trails form a basis for accountability within the organisation by tracking who requested access, why the request was granted or denied, and who approved the request.
- During investigations, audit reports can be used to conduct thorough analysis of incidents.

Audit trail – Best practices

- Live application connections and data should be subject to strict change control. When programs are changed, an audit log containing all relevant information should be retained
- An audit trail of all access should be securely maintained and reviewed on a daily basis.
- The audit log and issues related to the usage of sensitive privileges / utilities should be reviewed weekly and followed up for any inappropriate usage.
- The use of sensitive utilities should be logged in "tamper-proof" logs for review by the Systems Security Administrator, wherever possible.
- The router , firewall , switches audit logs should also be reviewed on a daily basis for unauthorized access

Audit Trail Analysis

- The audit trails need to be analyzed to determine vulnerabilities, establish accountability, assess damage and recover the system.
- Manual analysis of audit trails though cumbersome is often resorted to because of the difficulty to construct queries to extract complex information from the audit logs.
- There are many tools that help in browsing the audits.
- The major obstacle in developing effective audit analysis tools is the copious amounts of data that logging mechanisms generate

Approach to design secured applications

Custom Application development

Develop security controls throughout the SLDC.

- Provide adequate security training to those designing and developing applications (Stakeholders, Project Managers, BA's, Architects, Coders and testers.)
- Undertake application security review such as design reviews, code reviews & Penetration Testing at various intervals during the SLDC – not two days before go live.
- Develop Policies, Standards for Systems Development & Maintenance.
- Develop Policies and Standards for control of the Development Environment, Source Code and Access Control.
- Develop reusable SECURE code blocks.

Managing information security in enterprise applications – Holistic approach

Operate/Maintain

Vulnerability scanning regularly performed during the application maintenance phase on both the application and infrastructure to ensure no new security risks have been introduced and that the level of security is still intact

Requirements

Defined according to governance rules for authentication, authorization, non-repudiation, data confidentiality, integrity, accountability, session management, transport security, privacy, etc.

Governance

Security Polices, Guidelines, Standards, Procedures, Metrics created & enforced by organizations

Deployment

Application should be tuned and hardened at all layers of the platform stack to minimize infrastructure software misconfiguration vulnerabilities.

Design

Design with considerations for network, server, middleware, database and programming platform vulnerabilities, leveraging techniques such as threat modeling, risk analysis, misuse and abuse cases.

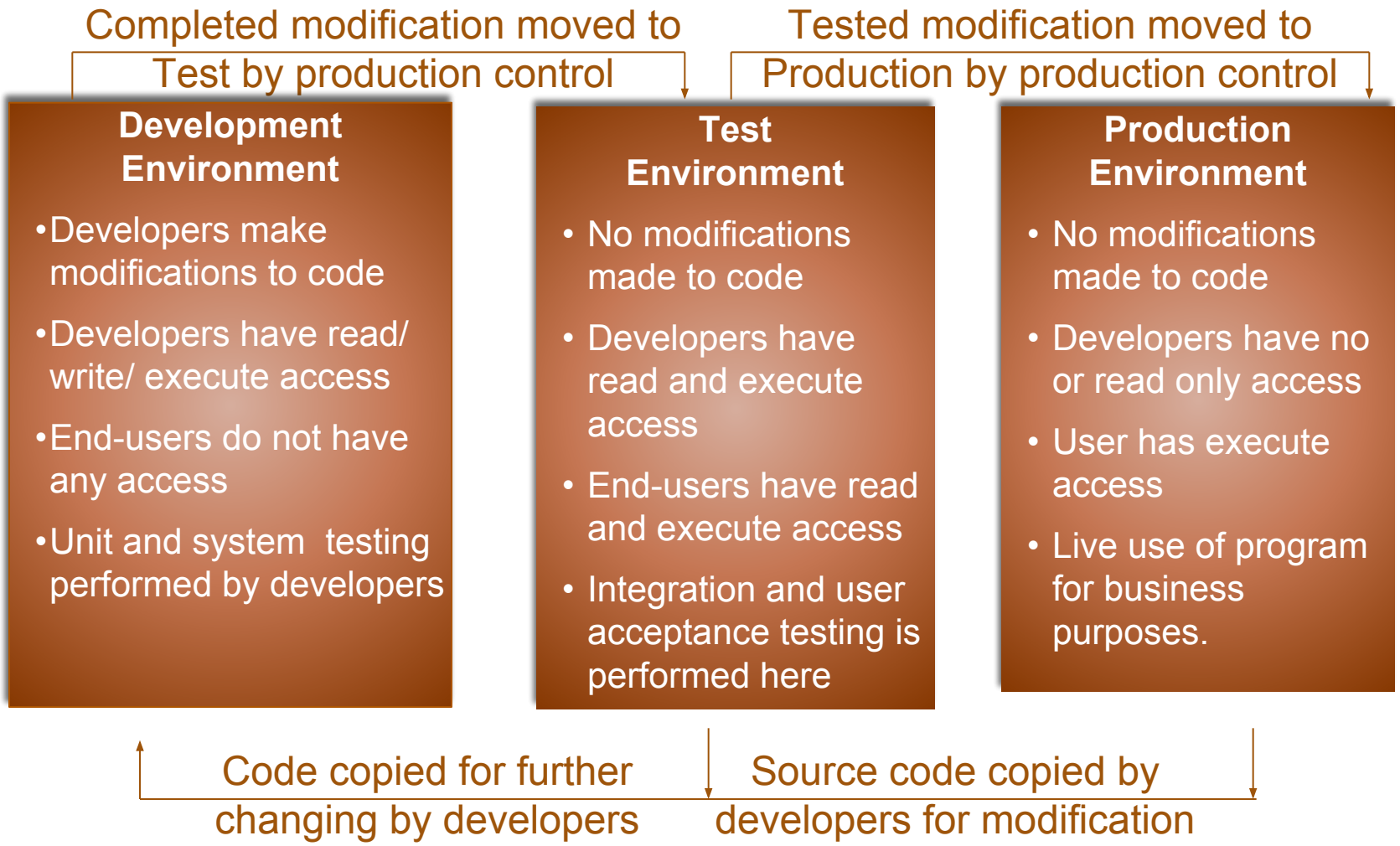
System & Integration Test

Penetration Testing performed during SIT to simulate application abuses and ensure any vulnerabilities uncovered are properly addressed as “security bugs”

Coding & Unit Test

Follow secure coding guidelines. Perform code review & code scanning to minimize coding vulnerabilities.

Enterprise Application – Important Security measures



Security Checks in Production vs. Development

Production Phase

- Testing is more end-to-end, checks application layer, network layer, and system layer security vulnerabilities
- Appropriate for tool-based vulnerability scanning
- Inappropriate for security functionality test & attack script penetration, due to lack of intimate application knowledge
- Good at finding commonly known platform vulnerabilities
- Not very good at finding application code specific vulnerabilities
- High cost related to late discovery of security defects

Development Phase

- Testing is more focused on application layer vulnerabilities
- Appropriate for all levels of security tests
- Very appropriate for security functionality test & attack script penetration, thanks to intimate application knowledge
- Good at finding commonly known platform vulnerabilities as well as application code specific vulnerabilities
- Low cost due to early discovery of security defects

End of Session