PV222
Security Architectures

Lecture 5

Identity Management

Course Outline

- *Session 1*: Defining and understanding the key problems in Identity Management.
- *Session 2*: What is an Identity, and what are its potential applications.
- *Session 3*: What are the challenges for managing a Digital Identity.
- *Session 4*: Process and procedural management.

Session 1

Defining and understanding the key problems in Identity Management

Session 1: Outline

- Who am I?
- Legal and Regulatory Imperatives
- Identity Theft

Definition

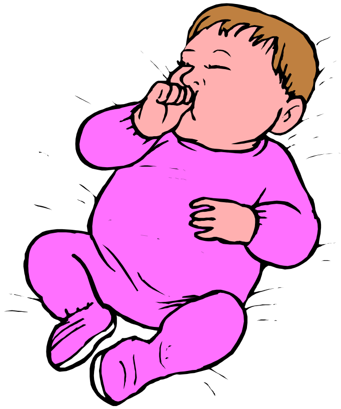
“Identity Management can be defined as the set of processes, tools and social contracts surrounding the creation, maintenance, utilisation and termination of a digital identity for people or, more generally, for systems and services to enable secure access to an expanding set of systems and applications.”

An Introduction to Identity Management

Jan De Clercq and Jason Rouault

June 2004 – HP White Paper

Who am I?



- While joined by umbilical cord, there is undeniable proof you are your mothers offspring.
- Once cord is cut, “proof” of identity relies on (removable) tags plus procedures.

The Jackal

- In Frederick Forsyth's novel *The Day of the Jackal* the would-be assassin of General de Gaulle escapes detection through the generation of a false identity:
  - He assumes the identity of a dead child by obtaining the child's *birth certificate* and using it apply for a *passport*.
- The procedure - often referred to as the "Day of the Jackal technique" has been exploited in many real crimes.

Lord Buckingham – I

- Christopher Edward Buckingham had used the name of a dead baby for 23 years.
- He stole his name from the birth certificate of a baby who died 20 years previously.
- The real Christopher Buckingham was born in 1962 and died a year later
- Arrested in Dover in January 2005.
- During interviews he admitted assuming a false identity but refused to reveal his true identity.

Lord Buckingham – II

- Jailed in Nov 2005 for 22 months.
- His former wife and two children also did not know his true identity.
- He daughter decided to try and track down his true identity.
- In May 2006, it was discovered that he was missing American ex-serviceman called Charles Albert Stopford III.
- He was then due to be deported to the US.

Regulation

- Industry regulation:
  - Health Insurance Portability and Accountability Act of 1996 (**HIPPA**)
  - **Sarbanes-Oxley Act** of 2002 (also known as the Public Company Accounting Reform and Investor Protection Act)
  - **Gramm-Leach Bliley Act** of 1999 (also known as The Financial Modernization Act)
  - Basel Accord, including Basel I and **Basel II**.
  - …

HIPAA – Privacy Rule

- From a US Gov website:
  - Q: "*Generally, what does the HIPAA Privacy Rule require the average provider or health plan to do?*"
  - A:
    - "*Notify patients about their privacy rights and how their information can be used.*
    - *Adopting and implementing privacy procedures for its practice, hospital, or plan.*
    - *Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.*
    - *Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.*
    - …"

HIPAA – Security Rule

- The Security Rule within the HIPAA regulation lays out three types of security safeguards required for compliance:
  - **Administrative safeguards**:
    - Policies and procedures designed to clearly show how the entity will comply with the act.
  - **Physical safeguards**:
    - Controlling physical access to protect against inappropriate access to protected data.
  - **Technical safeguards**:
    - Controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.

Gramm-Leach Bliley Act – I

- The act includes provisions to protect consumers' personal financial information held by financial institutions.
- There are three principal parts to the privacy requirements:
  - Financial Privacy Rule
  - Safeguards Rule
  - Pretexting provisions

Gramm-Leach Bliley – II

- Financial Privacy Rule:
  - Governs the collection and disclosure of customers' personal financial information by financial institutions.
  - It also applies to companies, whether or not they are financial institutions, who receive such information.
- Safeguards Rule:
  - Requires all financial institutions to design implement and maintain safeguards to protect customer information.
  - Applies not only to financial institutions that collect information from their own customers, but also to financial institutions "such as credit reporting agencies" that receive customer information from other financial institutions.

Legislation – I

- EU Directive:
  - EC Data Protection Directive (95/46/EC)
    - Aims to harmonise the national laws of the Member States.
    - Disparities between the laws of Member States for the protection of privacy act as obstacles to the free flow of personal information throughout Europe.
    - Free flows of personal information are necessary for the exercise of the four “fundamental freedoms” guaranteed by the Treaty establishing the European Community.
- Electronic communications:
  - Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (2002/58/EC).

Legislation – II

- Example: UK
  - European Data Protection Directive:
    - Establishes minimum data protection requirements across 28 EEA countries.
  - Data Protection Act 1998:
    - Implements EU Directive 95/46/EC into UK law establishing the 8 principles.
    - Creates civil and criminal penalties for breach of the Act.
    - Empowers the Information Commission as UK supervisory authority.
  - Information Commissioner's Office:
    - Responsible for UK policy, supervision and enforcement for data protection.
    - Issues decisions, enforcement notices, guidance, codes of practices etc.

Legislation – III

- **Data Controller** must ensure that processing:

1. Fair and lawful
2. For limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept longer than necessary
6. In accordance with data subject rights
7. Secure
8. Not transferred to countries without adequate protection

Legislation – IV

- **Data Controller** can demonstrate compliance controls through:
  - Documented data protection objectives
  - Defined roles and responsibilities
  - Clear internal policy framework
  - Internal training and awareness
  - External fair processing notices
  - Ongoing monitoring and review

Legislation – V

- USA:
  - Industry legislation:
    - HIPAA (Health Care)
    - GLBA (Financial Services)
  - State Law:
    - California Online Privacy Protection Act 2003, Security Breach Notice.
    - Being adopted by 30+ states.
  - Federal:
    - Telemarketing Sales Rule (Do not call)
    - Electronic Communications Privacy Act

Legislation – VI

- APEC (Asia-Pacific Economic Cooperation):
  1. Preventing Harm
  2. Notice
  3. Collection limitation
  4. Uses of personal information
  5. Choice
  6. Integrity of Personal Information
  7. Security Safeguards
  8. Access and Correction
  9. Accountability (includes Due diligence in transfers)

Legislation – VII

- Common principles?
  - Give notice to the person about whom it is collection personal information, or even obtain consent to do so.
  - Only collect the minimum information necessary to carry out its functions or provide the service involved.
  - Identify the primary purpose of collection and limit its uses and disclosures of the personal information to that primary purpose or related purpose.
  - Keep the information secure, complete, accurate and up to date, sometimes being required to subject itself to compliance audits.
  - Allow individuals to see all the information held about them and obtain correction of errors and sometimes be able to require deletion of unwanted information.
  - Deidentify or destroy personal information no longer in use.

Business Focus – I

- Brand Risk:
  - Risk to brand from privacy breach
  - Potential inconsistencies between policies and practices
- Employee Data Management:
  - Employees based around the globe and data distributed throughout the organisation
  - Requires localised and tailored approach
- Increased Regulation:
  - Multiple jurisdictions of privacy regulations
  - Legal solutions for EU data transfers such as Safe Harbor or model contracts
  - Managing relationships with Data Protection Authorities

Business Focus – II

- Customer Sensitivity:
  - Existing privacy policies and customer expectations
  - Multilingual and multicultural audience
  - Procedures for customer privacy complaints
- Extended Enterprise:
  - Relationships with partners, distributors, channels and resellers
  - Inconsistent implementation of privacy practices among independent organisations
  - Who has associated liability for privacy?
- Advances in Technology:
  - Web-based e-commerce application interact with customers online
  - Use of personalisation technologies such as cookies, smart tags, unique identifiers, customer profiles, etc.

Identity Theft – I

- **Identity theft** (or **identity fraud**) occurs when someone wrongfully acquires or uses another person's personal data, typically for their own financial gain.
- Techniques:
  - Stealing mail or rummaging through rubbish.
  - Eavesdropping on public transactions to obtain personal data.
  - Stealing personal information in computer databases.
  - Infiltration of organisations that store large amounts of personal information.
  - Impersonating a trusted organisation in an electronic communication.
  - Spam

Identity Theft – II

- Surveys in the USA from 2003 to 2006 showed a decrease in the total number of victims but an increase in the total value of identity fraud to US$56.6 billion.
- The 2003 survey from the Identity Theft Resource Centre found that:
  - Only 15% of victims find out about the theft due to a proactive action taken by a business.
  - The average time spent by victims resolving the problem is around 600 hours.
  - 73% of respondents indicated the crime involved the thief acquiring a credit card.

Identity Theft – III

- In Australia identity theft was estimated to be worth between AUS$1 billion and AUS$4 billion per annum in 2001.
- In the UK, the Home Office reported that identity fraud costs the UK economy £1.7 billion.
- Confusion over exactly what constitutes identity theft has lead to claims that statistics may be exaggerated.

Identity Theft – IV

- From Experian website:
  - Cases they had dealt with (up to June 2006):
    - It takes an average of 463 days for a victim to discover their details have been misused.
    - Average amount of credit gained fraudulently is £1921.80
  - Some of the ways in which they recommend you look after personal information:
    - Do not use “auto-complete” options in Internet browsers.
    - Taking care with WiFi and Bluetooth connections.
    - Taking care of portable storage devices (e.g. USB keyrings)

Session 2

What is an Identity, and what are its potential applications

Session 2: Outline

- Defining digital identities
- The main uses for an identity
- Authorisation
- Physical access control
- Technology from the business perspective
- Business issues

What is an Identity? – I

- Attributed Identity:
  - Given name
  - Date of birth
  - Place of birth
  - Parents name
  - Mother’s maiden name
  - … i.e. birth certificate

What is an Identity? – II

- Biographical Identity:
  - What you've done – education, qualifications.
  - Where you live(d).
  - What you do – employment.
  - Previous interaction with structured society.
- Biographical Data:
  - *Informal Def^{n}*: Any information that can be combined to identify an individual

What is an Identity? – III

- Biometric Identity:
  - Different types of biometrics
  - Accurate (?)
  - Intrusive
  - Requires technology
  - Useful for verifying post-enrolment

What is a Digital Identity?

- An identity of an individual can be broadly defined as the set of information known about that person.
- In the digital world a person's identity is typically referred to as their digital identity.
- A person can have multiple digital identities.
- Identities are not exclusively associated with people.
  - For example, they can be associated with services, systems and devices that could be used to act on behalf of people.
  - e.g. next generation mobile phones, DRM-based devices, etc.

Identities and Credentials

- A user may require multiple identities for multiple tasks:
  - Employee name/number for intra-organisational use.
  - Citizen has many different forms of identity for interacting with government.
  - A user of services (e.g. ISP) will usually have different identities for each service used.
- For each identity, the user must hold a credential, which the service provider uses to authenticate the user.

Privacy

- In some cases, the user who is making use of a service may wish to have a degree of privacy.
  - e.g. the user may not wish their identity to become known to other entities.
- In general, there are three aspects to privacy:
  - Anonymity
  - Pseudonymity
  - Unlinkability

Anonymity

- A user may wish to be able to access a service in an *anonymous* way.
- Anonymity means that no party will learn any of the identities of the user.
- Providing anonymity for free services is relatively simple.
- If payment is needed, then an anonymous payment system is needed, e.g. cash or e-cash.
- True (“absolute”) anonymity is difficult to achieve, since even revealing an IP address to some extent compromises it.

Pseudonymity

- Pseudonymity is a lesser form of anonymity, in which the user reveals a special type of identity to the service provider as a *pseudonym*.
- Typically, new pseudonyms will be generated regularly, i.e. pseudonyms are typically short-lived.
    - An example of short-lived pseudonyms is provided by the TMSIs used by GSM.

Unlinkability

- Unlinkability is a privacy property required to support the use of pseudonyms.
- Two pseudonyms are unlinkable if a third party cannot tell whether or not they belong to the same user.
- In practice, absolute unlinkability is often difficult to achieve, since the authorisation process may reveal information about the user.

Why De-identification is hard – I

- **De-identification**:
  - Most commonly used to refer to the process of removing or altering data in a medical record that could be used to identify the patient.
  - Technique employed to allow research, training, or other non-clinical applications to use real medical data, without compromising patient privacy.
  - Has become more urgent with the passage of HIPAA.

Why De-identification is hard – II

- For patient data, techniques involve:
  - Personal identifiers removed.
  - De-localisation.
  - Record order scrambling
  - Numeric items banded, extremes truncated
  - Dates reduced
- Not restricted to medical data:
  - In August 2006 AoL released (supposedly de-identified) search queries carried out by ½M customers over a 3 month period.
  - AoL pulled the dataset when people started looking at the data to see if it might be identifiable… but there are copies out there…

The Main Uses for an Identity

- Identification – its use in registration
- User authentication – the cornerstone of most computer security
- Identity verification – passports, ID Cards, etc.

Identification

- Identification:
  - Verification of the credentials held by an individual.
  - Secure creation of the digital entity bound to that identity.

Authentication

- Authentication:
  - Using some process or procedure to verify the validity of a claimed identity.
  - Binding the claimed identity to the one which is was originally linked.

Why Authenticate?

- In real life authentication is usually carried out prior to some action:
  - A bank clerk asks for identification before cashing a cheque.
  - A hire company employee will request to see a driver’s licence before handing over the keys to a hire car.
- In any automated system, the principle is the same: **Authentication** is generally a precursor to **Authorisation**:
  - You enter your ATM card and type in your PIN number to the ATM before you are allowed to withdraw money.
  - You enter your username and password to a computer before you can access files, printers and other resources.

Processes That Require Authentication

- The need for identifying human users of systems is clear, and covers many different application domains.
- For example, identity verification is required for:
  - controlling access to computers,
  - checking identification of a user in a library before charging out books,
  - limiting access to building and secure areas within buildings,
  - controlling the use of banking and e-commerce activities.

Application Domains – I

- The application domains will vary accordingly to the applicability of the enabling technology. Here are some suitable domains for biometrics:
  - Physical access control
    - To high security areas
    - To public buildings or areas
  - Time and attendance control
  - Identification
    - Forensic person investigation.
    - Social services application, e.g. immigration or prevention of welfare fraud.
    - Personal documents, e.g. electronic drivers licence or ID Card.

Application Domains – II

- Access Control
  - To devices:
    - Cellular phones
    - Logging in to computer, laptop, or PDA
    - Cars
    - Guns, gun safes
  - To local services:
    - Debiting money from the cash dispenser
    - Accessing data on smartcard
  - To remote services:
    - E-commerce
    - E-business

Remote Working – I

- Main goals of remote working are to cut costs and allow staff a better work/life balance.
- Financial benefits:
  - Reduced office space and travel time.
  - Audio, video and Web conferencing can reduce the need for travel.
- Financial costs:
  - Start-up cost of enabling technology.
  - Possibly home office furniture, equipment and insurance.

Remote Working – II

- Domestic broadband is increasing the reliability and availability of remote working.
- However, machines connected to an Asymmetrical Digital Subscriber Line (ADSL) are more likely to be targeted by hackers.
- VPNs are the standard technology for connecting in to the corporate network.
- Remote Access Servers (RAS) are commonly used on the corporate network to manage authentication, authorisation and accounting (so-called triple-A) functions.

Remote Working – III

- The corporate security policy might need to be amended to securely manage remote equipment, connections and data.
- Data Access:
  - The organisation might have legal obligations on data stored remotely – e.g. under the Data Protection Act.
  - This could impact your Identity and Access Management deployment.

VPN – I

- A Virtual Private Network (VPN) is a communications channel set up to communicate confidentially over a publicly accessible network.
  - A VPN consists of two parts:
    - The protected network, which provides physical and administrative security to protect the transmission.
    - The "outside" network (usually the Internet) which is less trustworthy.
- Generally use cryptographic protocols to provide:
  - Confidentiality
  - Sender authentication
  - Message integrity

VPN – II

- A well-designed VPN can provide the following benefits:
    - Extended geographic connectivity.
    - Increased security through encrypting traffic.
    - Reduced costs when compared to leased-lines.
    - Support users who wish to telecommute.
- However, VPNs extend the corporate infrastructure with ease, there are security implications, such as:
    - Client-side security must be tightened and enforced.
    - The scale of the “inside” network which can be accessed might need to be reduced.
    - Security logging on the corporate LAN might need to be adjusted to accommodate the VPN.

Single Sign-On (SSO) – I

- Authenticating to multiple systems is unpopular with users.
- Left to themselves, users will reuse the same password to avoid having to remember many different passwords.
- For example, users become frustrated at having to authenticate to a computer, a network, a mail system, an accounting system, etc.
- The solution for this frustration is called **single sign-on** (SSO).

Single Sign-On – II

- A user authenticates once per session, and the system forwards that authenticated identity to all other processes that would require authentication.
- Obviously, the strength of the single sign-on can be no better than the strength of the initial authentication.
- Also, the quality diminishes if someone compromises that first authentication of the transmission of the authenticated identity.
- Trojan horses, sniffers and wiretaps, man-in-the-middle attacks, and guessing can all compromise single sign-on.

Single Sign-On – Background

- SSO is not a new concept:
  - RACF (Resource Access Control Facility) from IBM, which was first released in 1976, managed user passwords for multiple applications.
  - Kerberos, developed in the 1980s, was a system to user authentication to multiple network services.

Kerberos

- Kerberos was designed as part of Project Athena at MIT.
- Designed to provide a means to authenticate workstation users (clients) to servers (and vice versa).
- Kerberos makes use of two types of Trusted Third Party:
  - An authentication server (AS)
  - A ticket-granting server (TGS)
- Idea of having two TTPs is that a user only needs load their long-term secret key into the workstation for the minimum time.

SSO and Identity Management

- In much of the open literature, SSO and Identity Management are becoming increasingly related concepts.
- In fact, SSO schemes often form the basis of identity management systems.
- However, in reality, there is no requirement for an Identity Management system to provide its services via SSO.
- In general Identity Management is a broader term, used to encompass much more than just the means of providing authentication services for users.

Advantages of Single Sign-On – I

- *Usability*:
  - The user no longer has to maintain credentials for each system/service.
  - Moreover, they do not have to do so *securely*.
- *User Management*:
  - In certain types of SSO schemes, a supporting management system can enforce a global policy.
  - Possibly allows for unifying rules and trust relationships among different entities.
  - Potential for reducing costs in a corporate environment. e.g. users can be added to, or removed from, the system through the granting (or revocation) of a single credential.

Advantages of Single Sign-On – II

- *Security*:
  - SSO has the potential to increase the overall level of security.
  - From the user perspective, it is arguably easier to securely maintain only one set of authentication credentials.
  - From the system/service's perspective, a globally enforceable policy can potentially mitigate the threat of human error.
  - However, having only one authentication credential for many services also poses a risk – if compromised the attacker can access all services.

An Architectural Overview – I

- An SSO scheme allows a user to authenticate themselves to more than one system/service using only a single authentication credential.
- A real-world system has to incorporate the life-cycle management of the identifiers by which the user is known to each system/service.
- Virtually all existing SSO schemes depend on the notion of authentication *sessions*.
- To start a session, the user needs to authenticate themselves to an *Authentication Service* (AS).

An Architectural Overview – II

- If the initial authentication is successful then, for as long as the session lasts:
  - The AS provides automatically logs the user into the systems/services they are registered with.
- The details of this are scheme dependant.
- However, in all schemes, it involves the AS, and possibly the user, executing a protocol with the service.
- The objective of this protocol is to authenticate the user to the service in a manner that does not (necessarily) require further manual interaction from the user.

An Architectural Overview – III

- At some later point in time, the authentication *session* will be terminated.
- The reasons for termination will vary from system to system.
- Sessions are subject to policies of the AS, the service and the user.
- Reasons for termination may include events such as:
  - Extended periods of inactivity.
  - A maximum number of logins performed.
  - Time limit on the session.
- Once a session is terminated, the user has to re-authenticate to the AS to start a new session.

SSO and distributed computing

- Historically, SSO has been applied to managed environments, e.g. within a large company.
- Company provides SSO as a “security layer” as part of the overall computing infrastructure.
- Products to provide SSO of this type are well-established.

Internet SSO

- Internet SSO refers to the ability of an Internet user to log in just once to an entity (local or remote), which then avoids the need for Internet Service Provider (SP) logins.
- Same reason as traditional SSO – to make life easier for user.
- However, apart from avoiding use of trivial or written down passwords, also addresses a trust issue not arising in the corporate environment.
- If same password used with multiple SPs, this potentially enables one SP to impersonate user to another SP.

Web Services – I

- The W3C defines a Web service as a software system designed to support interoperable machine-to-machine interaction over a network.
- A loosely coupled set of standards to allow services to be defined and found on a network.
- Core standards:
  - SOAP: Message envelope format.
  - WSDL: Service interface description format.
  - UDDI: Protocol for publishing and discovering services.
  - WS-Security: Defines cryptographic primitives (encryption and signature) for web services.

Web Services – II

- There is a move to integrate Web service to identity management.
  - The goal here is to provide a verifiable identity that describes both the originator of a transaction (e.g. the end-user) and the Web service end-point involved in processing the transaction.
  - A web application, which initiates a series of Web service calls, inserts the user’s identity along with the identity of the particular Web service.
  - This allows for complete end-to-end transaction auditability.

Business Issues

- Dual protection and business enablement role
- Improve the way that user identities are managed.

Security/Business Issues

- Do you send and/or receive valuable information over insecure networks?
- Do you care if unauthorised people gain access to this information (and change it)?
- Similar questions for stored information.
- Do you need to be able to identify people remotely?

Why Use Identities – I

- Legal Requirements
- Audit
- Enabling: Internet-based business and collaborative frameworks.
  - Move away from Identity and Access Management being seen as protection commodity, deployed to deal with specific security issues

Why Use Identities – II

- Cost saving
- Single Sign On
- Protection against Identity Theft. Identity theft is at an all time high. Companies need to protect themselves from exposure and do away with insecure, password-based authentication.

Business Benefits of IdM

- Some business benefits of implementing identity management:
  - Simplification of administration, thereby reducing administrative costs.
  - Increased security through investment in strong authentication mechanisms which can be used across the organisation.
  - Greater access to information by partners, employees and customers.
  - Singe Sign-On to hosted service providers, making such services more transparent for users.
  - Higher levels of regulatory compliance through the implementation of security, audit and access policies.

Session 3

What are the challenges for managing a Digital Identity

Session 3: Outline

- How should an organisation manage a digital identity?
- How do organisations want individuals to manage their identities?
- Government initiatives
- Legacy problems
- Cultural differences
- Determine the impact of an ineffective identity solution
- Design considerations and practical issues
- Open issues…

Requirements to Prove Identity

- *Validity*:
  - Is there sufficient supporting evidence to confirm that a person of that name exists.
- *Verification*:
  - Can you establish whether the applicant is the “data subject” or “owner” of the valid identity references.

Requirements for authentication

- Test “validity” by:
  - Accessing a wide range of data
  - Examining the history of the data
  - Evaluating the quality of the data
- How do we verify that “this is John Smith”?
  - Test “verification” by:
    - Verifying that only the genuine “data subject” would know e.g. pervious address – marital status – time in employment – time at current address – …

Electronic v Documentary Evidence

- Some credit reference agencies prefer electronic to documentary evidence.
- They consider documentary evidence to not be robust because…
  - How do you "reconstruct" the visual check of the document?
  - Data on documents is relatively static.
  - Logistics of a centralised checking process.
  - Documents easily forged/bought.
  - Genuine documents easily obtained falsely.
  - Documents used to breed other documents.
- Setting up multiple, corroborative, long-term electronic data sets should be more difficult…

Registration and Enrolment

- Registration issues:
  - It is crucially important
  - The registration process should be fit for purpose – what are you trying to protect?
  - Registration = Identification + Enrolment + …
  - Reliance (and any potential over-reliance) on the resulting system.
  - High-assurance registration and enrolment procedures do not scale well.
  - Do not forget the insider threat.

Security of Enrolment

- An example…
- Requirements for biometric enrolment:
  - Secure enrolment procedure.
  - Binding of the biometric template to the enrolee.
  - Check the template quality and matchability.
  - *Other requirements?*

Sample Enrolment Requirements

- Verisign have an authentication and verification procedure for SSL Certification.
- Process for confirming that:
  - The organisation is still in business.
  - The organisation owns/has rights to use the domain name listed in the common name of the Certificate Signing Request.
  - The corporate contact works for the organisation.
  - The corporate contact is aware of the certificate request.
  - The technical contact listed is authorised to receive the Digital ID.

Deployment Models – I

- Identity management systems are predominantly deployed in one of the following three models:
  - Silos; Walled gardens; Federations.
- Silo:
  - Identity management environment is put in place and operated by a single entity for a fixed user and resource community.

Deployment Models – II

- Walled Gardens:
  - Represent a closed community of organisations.
  - A single identity management system is deployed to serve the common user community of a collection of businesses.
  - Most frequently occurs in business-to-business exchanges.
  - Specific operating rules govern the entity operating the identity management system.

Deployment Models – III

- Federated identity management:
  - Emerging model, includes systems such as the Liberty Alliance.
  - The central different between federated identity systems and walled gardens is that there is no single entity that operates the identity management system.
  - Federated systems support multiple identity providers and a distributed and partitioned store for identity information.
  - Most systems exhibit strong end-user controls over how identity information is disseminated amongst members of the federation.

Identity Management Components

- Identity Management Systems can comprise a number of service and system components.
- These can be broken down into the following categories:
  - Data Repository Components
  - Security Components
  - Lifecycle Components
  - Consumable Value Components
  - Management Components

Data Repository Components

- Directory services and meta-directories:
  - These deal with the storage and management of identity information.
  - Provide standard APIs for access to the information.
  - Often implemented as an LDAP accessible directory, meta-directory, virtual directory or database.
  - Policy governing access to the information is generally stored here as well.

Security Components – I

- Security can be broadly broken down into the following three categories:
  - Authentication Provider; Authorisation Provider; Auditing Provider.
- Authentication Provider:
  - Also termed Identity Provider.
  - Primary authentication of an individual.
  - Generates an authentication token:
    - e.g. smartcard, biometric scan, X.509 certificate
    - The strength of the mechanism used will be application dependent.

Security Components – II

- Authorisation Provider:
  - Enforces access control when an entity accesses an IT resource.
  - Allow applications to make authorisation and other policy decisions based on privilege and policy information:
    - e.g. simple OS-driven access control, or more complicated systems such as RBAC.
- Auditing Provider:
  - Provides the mechanism to track how information in the repository is created, modified and used.
  - Can be used to in analysis in the event of circumvention of policy controls.

Lifecycle Components – I

- Lifecycle components can broadly be broken down into the two following categories:
  - Provisioning; Longevity.
- Provisioning:
  - The automation of all the procedures and tools to manage the lifecycle of an identity:
    - Creation of the identifier
    - Linkage to the authentication providers
    - Setting and changing attributes and privileges
    - Decommissioning the identity
  - In large systems, these tools generally allow some form of self-service for creation and management of an identity.

Lifecycle Components – II

- Longevity:
  - Creation of the historical record of an identity.
  - These tools allow the examination of the evolution of an identity over time.
  - Linked to the concept of *attestation* – the ability to attest what actors had access to what resources in what timeframe.

Consumable Value Components – I

- These can be broken down into the following three categories:
  - Single Sign-On (SSO); Personalisation; Self Service.
- Single Sign-On:
  - Allows a user to perform a primary authentication once.
  - This then allows them to access the set of applications that are part of the identity management environment.

Consumable Value Components – II

- Personalisation:
  - Also called preference management tools.
  - Allow application-specific, as well as generic information, to be associated with an identity.
  - Allow applications to tailor the user experience.
- Self Service:
  - Enable users to self-register for access to business services and manage profile information without administrator intervention.
  - Allows users to perform authentication credential management:
    - Assigning and resetting passwords
    - Requesting X.509 certificates, etc.

Management Components – I

- Can be broken down into the following four components:
  - User Management; Access Control Management; Privacy Management; Federation Management.
- User Management:
  - Provides centralised infrastructure for managing user profile and preference information.
  - Allows organisation to decrease overall IT by providing:
    - User self-service capability.
    - Directory optimisation.
    - Profile synchronisation.

Management Components – II

- Access Control Management:
  - Centralised infrastructure for managing user authentication and authorisation.
  - Allows automating access policies for employees, customers, and partners.
- Privacy Management:
  - Implements privacy and data protection policies.
- Federation Management:
  - Enables the establishment of trusted relationships between distributed identity providers.

Federated Identity Management

- Federated v Local Identity
- Identities Change:
  - Marriage
  - Multiple names
    - Bill/William – Jon/Jonathan – Andy/Andrew – …
- People move:
  - Updating information
  - Notification to federator

Federated Identity Management – I

- *Federated Identity*:
  - Allows multiple organisations to exchange and link identity information across organisational boundaries.
  - This could be between partner, supplier or customer organisations.
- A federated identity management system is one that provides a bridge between segregated silos of identity systems.

Federated Identity Management – II

- Drivers for Federated Identity:
  - A Service Provider (SP) may wish to accept the identity of their customers – who will in turn be the Identity Provider (IdP).
  - Organisations (IdPs) may want to extend their employee “identities” to their third-party service providers.
  - Roles, credentials or even authorisation policies may be asserted from the IdP to the SP.
  - Multiple SPs may wish to make use of the authentication mechanisms of a single IdP.

Federated Identity Management – III

- Drivers for Federated Identity (cont.):
  - A large organisation which needs to manage numerous security domains simultaneously may wish to build an Internal federation across traditional identity silos.
  - This can lead to providing cross-domain SSO without having to homogenize systems or authentication approaches.

Federated Identity Management – IV

- Partners in a federated management solution also need to consider policy adherence, for example:
  - Access policies that define acceptable levels of access agreement.
  - Privacy policies according to the industry and technical deployment requirements.
  - Logging of events for audit, compliance, etc.
  - Risk and liability agreements.
  - etc…

The Liberty Alliance – I

- The Liberty Alliance (www.projectliberty.org) is a consortium of over 140 different companies, recently developed a set of open specification web-based SSO.
- It has published a series of specification for an “open” XML-based SSO system.
- The user is known as a *Principal* and the Authentication Server as the *Identity Provider* (IP).
- A user authenticates to a Liberty IP. The IP then automatically authenticates the user to other Service Providers.
- User then needs only one password (or other means to authenticate to IP).

The Liberty Alliance – II

- The key Liberty objectives are to:
  - Enable consumers to protect security and privacy of their network identity information.
  - Enable businesses to manage customer relationships without third party involvement.
  - Provide an open SSO standard including decentralised authentication and authorisation from multiple providers.
  - Create a network identity infrastructure supporting all network access devices.

The Liberty Alliance – III

- They make use of SAML (Security Assertions Markup Language) to exchange authentication and authorisation information.
- Liberty uses “trust circles” which are formed from trusted ASs and sets of services.
- The first authentication is from the user to the AS, who then sends assertions, containing “name identifiers” to the service.
- These name identifiers must be constructed using pseudo-random values and are therefore potentially unlinkable.

The Liberty Alliance – IV

- However, the unlinkability can be compromised in a number of ways:
  - The AS knows all the user identifiers, and services could collude with the AS to link the pseudonyms to the users.
  - Services might be able to correlate SSO identities based on network addresses (although this issue can be addressed by means discussed earlier).
  - Profile information that each service maintains (tel no, credit cards, etc) can also be linked to user identifiers.
- The Liberty Alliance specification is independent of the specific user authentication mechanism used by the AS.
  - The details of the specific mechanism are explicitly stated in the assertion.

Microsoft's InfoCard

- InfoCard is a Microsoft architecture for identity management.
- It has a number of component parts:
  - A distributed architecture for identity management.
  - A set of defined Web Services interfaces between entities in the architecture.
  - A set of software which will become available both for Vista and SP which will enable users to manage their identities in a Windows environment.
  - Development support to enable applications to use InfoCard managed identities.

Identity Metasystem

- Microsoft refers to this collection of components as an Identity Metasystem.
- The idea is to provide a unified way for (Windows) users to use many different underlying identity management systems.
- Key ideas here are:
  - Provide a simple user model for identity.
  - Enable users to control which identity is used for what purpose.

What about Passport?

- Microsoft’s experience with Passport has been rather painful.
- They tried to solve the problem of identity management by becoming the global identity provider.
- This idea failed – the main lesson is that there will never be such a global identity provider.
- This has led to InfoCard, as a means of supporting an identity ecosystem with multiple providers…

The Identity Problem

- The Internet has arisen without any unified notion of user identity.
- As a result, there are many different solutions in place for managing identities.
- Almost every website has a different way of managing login, and collecting various bits and pieces of personal information.
- As a result, various solutions to identity management (notably SSO schemes) have emerged.

Criminality and Identity

- Serious threats to identity have emerged, notably phishing and pharming attacks.
- Problems arise because users do not know who their PC is talking to.
- Users are tricked into revealing credentials and/or installing malicious software.
- In parallel, business holding multiple user identities are attacked, and identity data (e.g. credit card numbers) is compromised.
- Better ways of managing identities needed.

Identity Management is tough

- Currently, the only successful ID Management schemes are those for particular domains, e.g.:
  - Kerberos within companies.
  - Special-purpose PKIs for company use, and for specific systems (e.g. EMV).
  - Passport for MSN/Microsoft.
- No global schemes – no universal PKI.
- Identity is context-specific, which makes a universal global identity provider very unlikely.

Some Identity Definitions

- *Digital identity*: a set of claims made by one digital subject about itself or another digital subject.
- *Digital subject*: a person or thing, represented or existing in the digital realm.
- *Claim*: an assertion of the truth of something.

Comments – I

- The Microsoft definition of digital identity is a very general one, and does not distinguish between two concepts which are often treated separately:
  - Identifiers or labels (e.g. email address, National Insurance Number, passport number, …)
  - Attributes (e.g. the identity holder is an employee of company X, a silver card holder for airline Y, a season ticket holder for train route Z, …)

Comments – II

- There are two justification for the Microsoft "claims" approach:
  - It enables protocol interactions to be simplified – a single protocol can be used to transfer claims.
  - Some types of claim are difficult to categorise – a credit card number may be viewed as both an identifier and an attribute.
- However, on the down side, human beings by and large understand the distinction between the two types of claim – this means that it may be a useful distinction.

The Laws of Identity

- Microsoft has devised a set of seven Laws of Identity, which capture the philosophy behind InfoCard.
- In fact, if adhered to, these laws appear to have quite general repercussions for privacy in information systems.
- Rather grand claims are made for the general truth of these “laws”.

Law 1: User Control and Consent

Technical identity systems must only reveal information identifying a user with the user's consent.

- Success of a system requires user trust, and giving users control will build trust.
- The law permits implementations where the metasystem allows the users to decide to automatically use identity information in a specific context.

Law 2: Minimal Disclosure

The solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution.

- This approach minimises risk by using the “need to know” principle.
- It also reduced risk of attack.
- This also means minimising use of global identifiers (as opposed to local identifiers).

Law 3: Justifiable Parties

Digital identity systems must be designed so [that] the disclosure of identifying information is limited to parties having necessary and justifiable place in a given identity relationship.

- The user must be aware of who he/she is sharing information with.
- This law is seen to explain the failure of Passport – Microsoft was not seen as a "necessary and justifiable" general purpose identity provider.

Law 4: Directed Identity

A universal identity system must support both “omni-directional” identifiers for use by public entities, and “uni-directional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

- A uni-directional identifier is essentially a pseudonym.
- In general, pseudonyms should be used unless there is a good reason not to.

Law 5: Pluralism of Operators and Technologies

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

- This is self-evident – we all use a multiplicity of different identities, with the choice of identity depending on the context – this is not going to change.
- A universal metasystem must clearly support all these types of identity.

Law 6: Human Integration

The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambigious human-machine communication mechanisms offering protection against identity attacks.

- The human user is a key component – the lack of human understanding of the PC interface (and the identities it displays) leads to phishing and pharming.

Law 7: Consistent Experience Across Contexts

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

- To support the previous law, users need a consistent view of identity across multiple applications.
- This consistency should be supported by the identity metasystem, and more generally by the user experience across applications.

The InfoCard architecture

- InfoCard defines three types of entity:
  - *Users/Clients*, i.e. the entities (digital subjects) for whom identities are managed.
  - *Relying Parties*, i.e. entities who wish to have some assurance regarding an identity for a user.
  - *Identity Providers (IPs)*, i.e. entities issuing identities and providing assurance regarding identities to Relying Parties.

Model operation – I

- The *service requester* is a client application running on the client (user) system.
- The *relying party* is the target service the user wishes to access via the service requester.
- One of more *identity providers* can issue security tokens (to support client application).
- The target service may optionally delegate authentication/validation of user identity to an *Authentication/Authorisation Security Token Service*.

Model Operation – II

- The user, interacting with the service requester via the *identity selector*, may have identities issued by one or more IPs.
- Each identity is represented by an *InfoCard*, which is the means by which the user interacts with the identity selector to choose which identity to use.
- Each IP runs a Security Token Service (STS), to generate security tokens.
- A *Self-issued Identity Provider* may be provided by a client platform to allow use of self-issued tokens.

InfoCard-Liberty Differences

- Clearly there are differences in *scope*. Notably, InfoCard addresses user identity management.
- However, there are clear overlaps and inconsistencies.
- Liberty provides profiles which work in the absence of identity management software on the client.
- InfoCard, by contrast, is built round client software.
- The existing Liberty profiles for the SSO and Federation Protocol are not consistent with InfoCard.

User Interface Issues

- A key component of the InfoCard architecture is the way that identities are presented to users.
- The objective is to provide a unified and simple way to manage user identities.
- This applies even when the identities rely on vastly different technologies.

InfoCards

- An InfoCard represents a single digital identity for a user issues by an IP.
- Multiple identities for the same user (from same IP) would give separate InfoCards.
- The InfoCard is not a security token used to carry identity claims – it simply represents the relationship with the IP.

InfoCard contents

- An InfoCard carries the IP’s issuing policy for tokens, including:
  - Token types it supports.
  - Claim types it handles.
  - The credential to use for user authentication.
- It must contain enough information about the IP’s capabilities to allow the identity selector to match it with the RP’s token requirements.
- The user can then select a suitable InfoCard from amongst those available.

Authenticating to the IP

- The InfoCard specifies the type of credential that must be used to authenticate the user to the IP.
- This must take place before any tokens are issued.
- A number of credential types are supported by InfoCard – we look at a few.
- User authentication protected using XML encryption and XML signature.

InfoCard – The Future…

- Identity management is a rapidly developing area.
- InfoCard, if it succeeds, could significantly improve identity security and privacy.
- However, it requires:
  - IPs and RPs to support web service based interactions.
  - User adoption of InfoCard interface, including registering with appropriate IPs.

Legacy Problems

- Large industrial manufacturer implemented a PKI to support authentication and encryption.
  - Rolled out in conjunction with employee badge.
  - Used to support SSL-based VPN.
  - Integration to existing back-end mainframe applications (50+) was difficult and incomplete.
  - Still have to support an existing OTP mechanism – double effort.
- When planning an IdM project, ensure that you factor in the applications you want to support.

Cultural Difficulties & Differences

- In Japan, internal vein pattern scans of fingers and palms are becoming popular for identity management.
  - Avoids the perceived law enforcement stigma of fingerprinting and is highly accurate.
  - The technology has yet to proliferate beyond Japan.
- Although facial recognition is not the most accurate, people are generally more comfortable with it than other forms of biometrics.

Impact of an Ineffective Solution – I

- An ill-designed identity management infrastructure might escalate costs by increasing the following:
  - time spent per day by staff logging on and authenticating to various applications;
  - time spent by administrative staff managing digital identities within the organisation;
  - the number of password re-sets required;
  - data redundancy – and the associated administrative costs – throughout the organisation.

Impact of an Ineffective Solution – II

- Inability to carry out function
- Reduced security
- Placement of liability
- Inability to charge for services:
  - If a client makes use of a service without the service provider being able to adequately identify them, then the provider cannot charge for the service.

Open Issues – I

- A number of issues need to be considered when discussing Identity Management solutions:
  - *Authenticity of identity*:
    - How do determine, and measure, the accuracy and validity of identity information?
    - How do you generate confidence in the identity information?
  - *Longevity of information*:
    - Can you track changes to identity information over time?
    - Can you provide the evidence to support historical investigation?

Open Issues – II

- *Privacy*:
  - Do you have adequate controls to preserve individual privacy?
  - Does the system provide adequate support for anonymity and multiple user controlled personas?
- *Identity Theft*:
  - Does your system make it easier to perpetrate identity theft of identity fraud?
- *Legal Structures*:
  - What protections are in place for the holder of the identity of for the relying party?

Session 4

Process and procedural management

Session 4: Outline

- Enrolment & registration
- Management of User Authentication
- Provisioning and de-provisioning services
- Administration and policy management
- Matching technical solutions to business requirements

Enrolment & Registration – I

- Enrolment
  - Face-to-face v Remote
  - PKI Levels (Class-I, class-II, etc.)
    - Various levels of identification
    - Various levels of liability
    - Various strengths of algorithm
  - Relate to processes:
    - Human error + process (ex: where judge criticised an organisation for not even having processes) **[GP]**
    - Banking (Know your customer regulation)

Enrolment & Registration – II

- Human Resources:
  - HR are the central authority until you arrive:
    - Rarely notified of anything after this.
  - To apply Federated Identity, then you need a process for checking that Mr X ≠ Mr Y.
  - HR might be the only people who can do this.
  - Observation:
    - HR put you on, but don’t take you off.
  - Federated v. Silo Concept (what happens in practice).

Example: Biometric Enrolment

- Process through which the user’s identity is bound with biometric template data.
- Involves data collection and feature extraction.
- Biometric template is stored in a database or on an appropriate portable token.
- There may be several iterations of this process to refine biometric template.
  - A live match of the enrolled template should be attempted to ensure that the template is a good representation.
- *Important to verify that the user is actually the person who they claim to be!*

Security of Biometric Enrolment

- Requirements for enrolment:
  - Secure enrolment procedure:
    - Who is authorised to add users to the system?
  - Binding of the biometric template to the enrolee:
    - Are you certain the biometric template cannot to replaced at a later time?
    - Who has access to any template database?
  - Check the template quality and matchability:
    - Any negative impact on biometric performance can have a knock on impact on security.
  - *Other requirements?*

Is everything OK?

Announcement in Microsoft Security Bulletin MS01-017

"VeriSign Inc recently advised Microsoft that on January 29-30 2001 it issued two VeriSign Class 3 code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee."

Management of User Authentication – I

- IdM Database issues:
  - Accuracy
  - Scalability
  - Extensibility:
    - The ability to upgrade the structure of the database simply after is has been set up.
  - Interoperability
  - Speed of Implementation
  - Solution Complexity
  - Data Ownership

Management of User Authentication – II

- Life-cycle Management
- Provisioning
- Workflow
- Password Management
  - Password reset
  - Systems Synchronisation issues
- Self-service administration
- Delegation

Lifecycle Management – I

- An identity life-cycle management process helps keep users' entitlements current throughout their career.
  - For example, as a user moves from HR to finance, the life-cycle process should remove access to data an applications for staffing and add privileges to financial apps and data.
  - These processes can be manual or automatic.
  - An automatic process is likely to be more timely ensuring that deletion and additions to privileges happen simultaneously.
  - Where is the source of the information feed?
  - How do you ensure timeliness in the start of the process?

Provisioning – I

- *Provisioning* is the notion of managing the information related to authentication and authorisation.
- Provisioning can be broken down into three areas:
  - Account provisioning; Resource provisioning; Account de-provisioning.
- Account provisioning:
  - Deals with identity-related information associated with individuals:
    - Adding an Identity; Modifying an Identity; Deleting an Identity; etc.
  - This includes their personal attributes, affiliations, etc.

Provisioning – II

- Resource provisioning:
  - Deals with business assets such as computers, databases and applications.
  - Manages the permissions associated with those assets.
  - Essentially the management of authorisations and privileges within the system.
- Account de-provisioning:
  - Deals with the termination of access rights to systems and services.
  - If not carried out in an accurate and timely manner it can leave an organisation open to additional risk.
  - Also deals with the re-allocation of those systems and services.

Provisioning – III

- Authoritative Sources:
  - Multiple authoritative sources may exist in an organisation:
    - HR feeds, systems providing financial data services, directories, etc.
  - It is important for an organisation to make one authoritative source the main source of identity information.
  - This will help prevent incorrect information being entered when an identity is created.
  - Receiving, validating, and updating information is important if you are to consistently manage identity information.

Workflow – I

- *Workflow* describes a means of controlling the identity provisioning process.
  - A request will be entered and routed via a predetermined path:
    - This allows those who are responsible to review and authorise the request to do so.
  - The request is then passed on to the entity who is responsible for creating the identity.
  - Requests are automatically routed to each participant in the process.

Workflow – II

- This should allow for the provisioning process to be applied consistently across all departments.
- It should also allow for a built in audit trail of the request to verify who was responsible for authorising different stages of the request.
- An automated workflow can be used to automatically notify the managers or administrators for approval of actions.
  - This can be useful when a workflow policy is linked to self-service administration for authorisation of user initiated requests.

Password Management – I

- Passwords are widely considered to be a weak form of authentication.
  - However, ease of setup and no additional hardware requirements mean that passwords are likely to be here to stay.
  - Secure management of the passwords you have becomes more important.
- Password management:
  - Establishing and managing password policies.
  - Changing or resetting passwords.

Password Management – II

- Password Synchronization:
  - Any update to the password information needs to be propagated quickly and securely.
  - This allows you to keep reduce the number of passwords that a user has to remember.
  - Update costs and administrative overheads can be kept to a minimum.
- Issues to consider:
  - Is the person requesting the password change the person they claim to be?
  - How do you deal with different password policies across different domains/silos?

Delegated Administration

- Typically, there are a select group of individuals (managers, administrators, etc.) who are authorised to create, modify, delete, etc. identity information.
- Delegation refers to the ability to pass on that administrative right to others who would not normally have the permissions to do so.
- This can be useful in a number of cases:
  - Where a partner organisation can be delegated the rights to manage their own employee data.
  - Where certain individuals in specific departments in a large organisation might only have hold privileges to modify the data on people within their dept.

Self-Service Administration

- In certain contexts it may be useful to allow the user who the identity refers to manage some aspect of that identity.
  - For example, if personal data (e.g. personal phone number) needs updating in the corporate database.
  - This can potentially reduce administrative costs and time.
- Where this might be done, there are certain issues to consider:
  - Which fields can be updated/changed.
  - Validity checking the data might be appropriate.
  - The update might actually start a workflow request which needs separate authorisation.

Matching Technical to Business – I

- Technical Deployment Considerations:
  - What are the application requirements?
  - Are you going to have to integrate to legacy systems?
  - What type of user authentication technology can you support?
  - Technical considerations might change depending on the different candidate technologies.
- Architecture/Infrastructure considerations:
  - Offline/online?
  - Heterogeneous platform?
  - Partner infrastructure/remote clients?

Matching Technical to Business – II

- Cost:
  - What is the total cost of ownership?
    - Passwords are very easy to set up, but password reset costs in large infrastructures can be high.
  - What other parts of the infrastructure will be affected?
    - Some organisations have used a stronger than necessary means of authentication to enable reduced costs through the use of leased line.
  - Size (Manual v Automated):
    - Often there is a cost no-mans land between the very small and the very large.

Which Biometric Method/Product?

- Sample considerations when considering deploying biometric authentication.
- Depends on the application:
  - reliability
  - security
  - performance
  - cost
  - user acceptance
  - liveness detection
  - users that are unsuitable
  - size of sensor