# SENG 460 / ECE 574
# Practice of Information Security and Privacy

Will cover Physical Security from last time

Week 8

Identity, Access Management

Logging, Policies, Standards, Audits, Compliance

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

# Key terms

- authentication — proof of identity – allows a user access to a system
- authorization — determines the privileges users will have
- username/password
- two factor (2FA), multifactor (MFA)
- two or more of:
  - something you know (e.g. password, PIN)
  - something you have (e.g. phone, hardware token)
  - something you are (e.g. biometrics like fingerprint, retina or iris, gait, typing pattern, facial recognition)

University of Victoria

# Access terms

- access request
  - access is needed
  - access request submitted
  - request is reviewed and approved/denied
  - request is implemented
  - requester notified

ensure separation of duties

ensure records of requests and approvals

who approves? usually manager or system/data owner or both

- employee identification cards vs. access cards
  - magnetic stripes, smart cards, proximity cards

University of Victoria

# Access terms

- credentials

  e.g. “any user name, identification number, password, license or security key, security token, PIN, or other security code, method, technology, or device used, alone or in combination, to verify an individual's identity and authorization to access and use the Services” (https://www.lawinsider.com/dictionary/access-credentials)

- identity proofing

  verifying claimed identity matches actual identity

- background checks

  e.g. employment, education, criminal records,

  credit history, motor vehicle and license record checks.

- issuing credentials

  e.g. providing credentials to a person or business

University of Victoria

# Onboarding/Offboarding

| | |
|---|---|
| onboarding | individual joining the organization |
| offboarding | individual leaving the organization |
| transfer between roles | individual changing jobs |
| provisioning | providing access |
| deprovisioning | removing access |
| requests, approvals | part of the access request process |

University of Victoria

# Key terms

- least privilege — person should have the minimum privileges or access to do their job, no more, no less
- job rotation — move people between jobs to limit fraud
- mandatory vacations — to reduce fraud
- privilege creep — gaining more access than you should have (aggregation of privileges)
- separation of duties — requiring more than one person to complete a task
- collusion — eg. two people working together to defeat SoD

University of Victoria

# Key terms

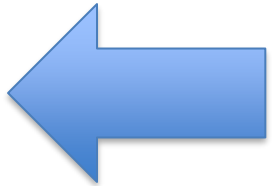
- password — string of characters used to authenticate access e.g. Summer2022
- passcode — often used interchangeably with password; may refer to a ‘pin’ e.g. 3141
- passphrase — longer string of text e.g. winteriscomingtomorrow
- password length — password must be X characters or more
- password complexity (e.g. upper, lower, numbers, punctuation, special chars)
- password aging — must change password after X days (password expiry)
- password history — can’t use the same password as last X times

# Identity

- Identity 2.0 Keynote – Dick Hardt

Watch this:

https://www.youtube.com/watch?v=RrpajcAgR1E (15 min)



Other:

https://www.youtube.com/watch?v=bBH-bZbnL5Q

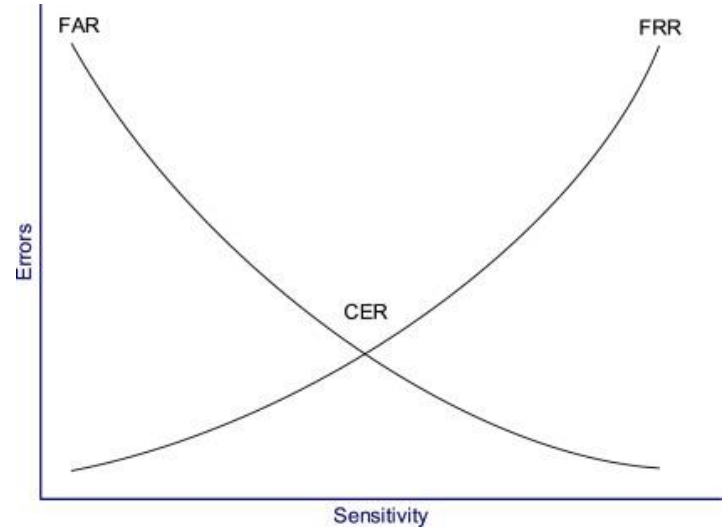
University of Victoria

# Review

- access control – allowing only authorized users, programs other computer systems to gain access
  - specify which users can access a system
  - what resources the users can access
  - what operations the users can perform
  - enforce accountability for user actions

# Review

- multi-factor authentication (2 or more of…)
  - something you know, something you have, something you are
- biometrics
  - fingerprints, retina, iris, vascular, gait, typing, voice, etc
- false accept/reject rates
  - false reject rate (FRR) - type 1 error - when authorized users are falsely rejected
  - false accept rate (FAR) - type 2 error - when unauthorized persons are falsely accepted
  - crossover error rate (CER) – point at which false rejection rates and false acceptance rates are equal – smaller the CER the more accurate the system




https://www.sciencedirect.com/topics/computer-science/crossover-error-rate

University of Victoria

# Tips

- maintain least privilege
  - should have the access they need to do their job – no more, no less
- centralized record of who has what access?
- regular review, separation of duties (SoD) violations
- identity management solution
  - knowledge of who has access to what
  - alerts, remediates discrepancies
  - maintains concept of roles
  - pros/cons (is it feasible to do for all systems?)

University of Victoria

# Review

Types of Controls:

1. **Administrative controls**: policies and procedures, disaster recovery plans, awareness training, security reviews and audits, background checks, review of vacation history, separation of duties, and job rotation.

2. **Logical or technical controls**: Restrict access to systems and the protection of information — Encryption, smart cards, anti-virus software, audit trails, log files, ACLs, biometrics, and transmission protocols (Kerberos, IPSec)

3. **Physical controls**: guards and building security, biometric access restrictions, protection of cables, file backups

# Access Rules

- Three types of access rules:
  1. Mandatory access control (MAC)
  2. Discretionary Access Control (DAC)
  3. Non-Discretionary Access Control

# Mandatory Access Control (MAC)

Authorization of subject's access to an object depends on labels (sensitivity levels), which indicate subject's clearance, and the classification or sensitivity of the object

a. Every Object is assigned a sensitivity level/label and only users authorized up to that particular level can access the object
b. Access depends on rules and not by the identity of the subjects or objects alone
c. Only administrator (not owners) may change category of a resource
d. Output is labeled as to sensitivity level
e. Unlike permission bits or ACLs, labels cannot ordinarily be changed
f. Can't copy a labeled file into another file with a different label
**g. Rule based access control**

**central security grants access to specific users**

# Discretionary Access Control (DAC)

Subject has authority, within certain limits, to specify what objects can be accessible

(e.g., use of ACL)

a. User-directed means a user has discretion

b. Identity-based means discretionary access control is based on the subjects identity

**c. Very common in commercial context because of flexibility**

d. Relies on object owner to control access

**e. Identity-based access control**

**data owner grants access to others as they choose**

# Non-Discretionary Access Control

Central authority determines what subjects can have access to certain objects based on organization's security policy

May be based on individual's role in the organization (**Role-Based**) or the subject's responsibilities or duties (task-based)

University of Victoria

# Role-Based Access Control (RBAC)

- restricting access based on roles
- notion of “employee” or “base” role – access everyone has

  (eg. Active Directory + LDAP)
- steps

  1) identify systems
  2) create library of roles
  3) assign users to defined roles

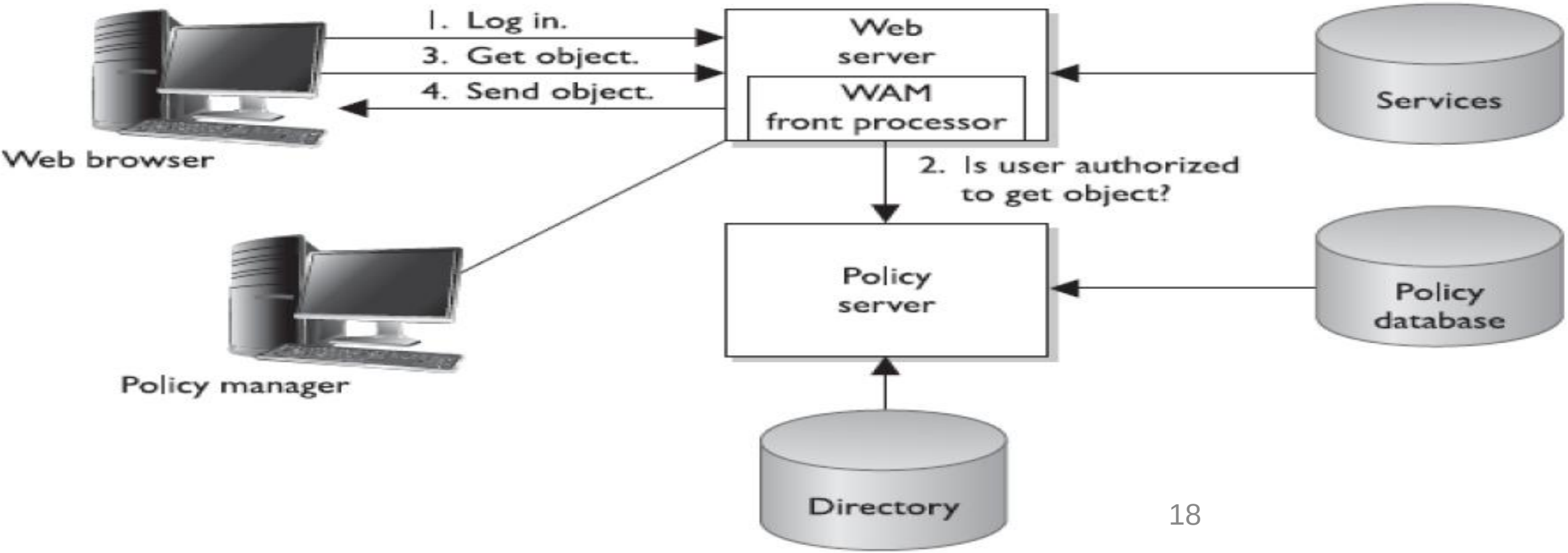
**Example**

role is a collection of permissions and/or other roles

also: ABAC (attribute based access control)

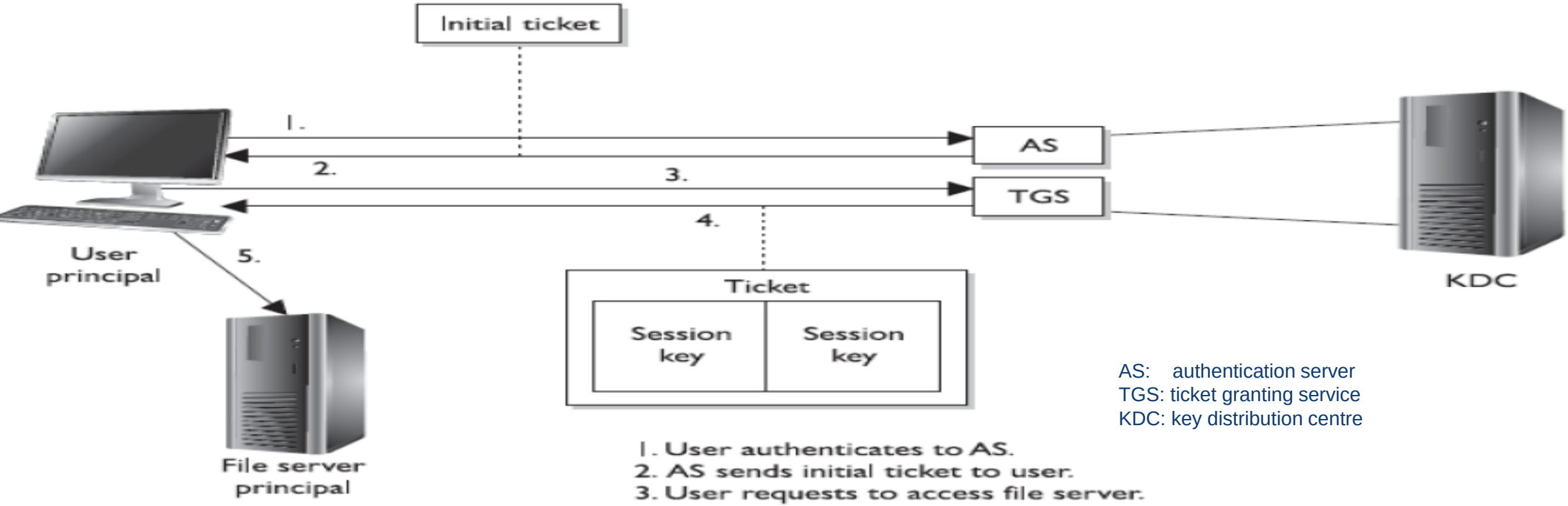
# Web Access Management

- software controls what users can access when using a browser to access a web-app



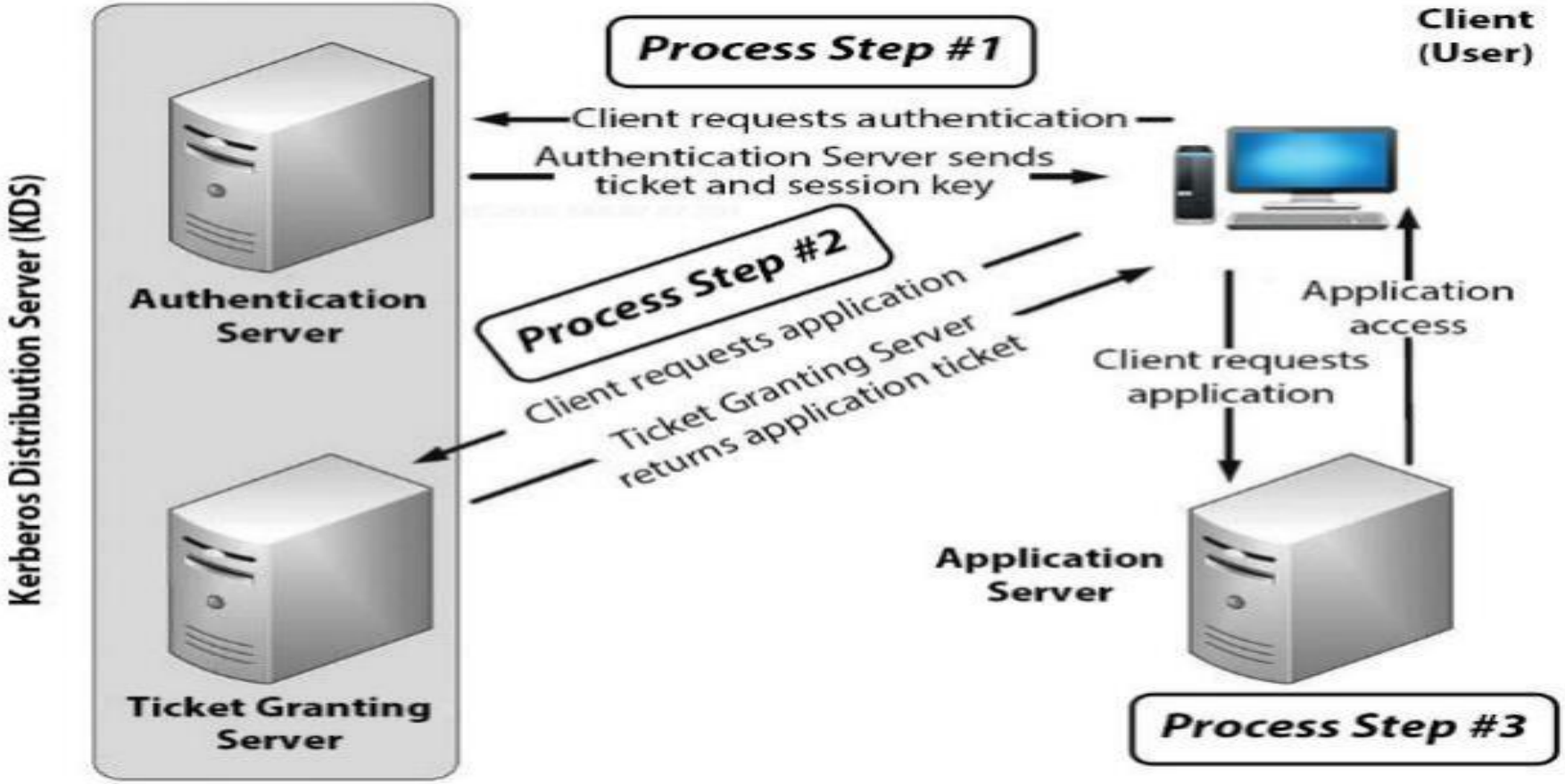
# Single Sign-on

- allows users to enter credentials one-time and access all resources in same domain (eg. Kerberos)

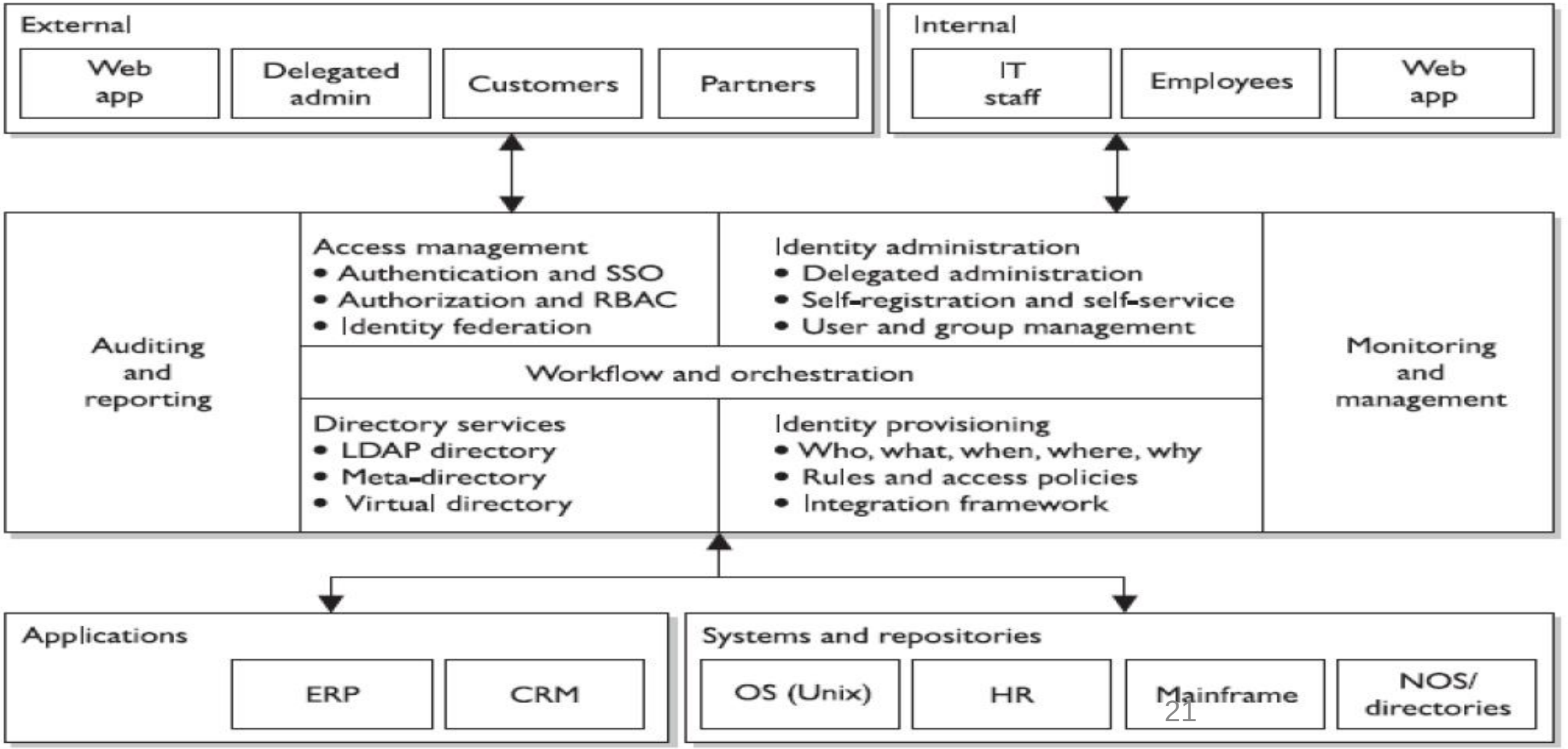


# Kerberos

- three components: authentication server (AS), ticket granting service (TGS), key distribution centre (KDC)



# Identity Management



# SAML

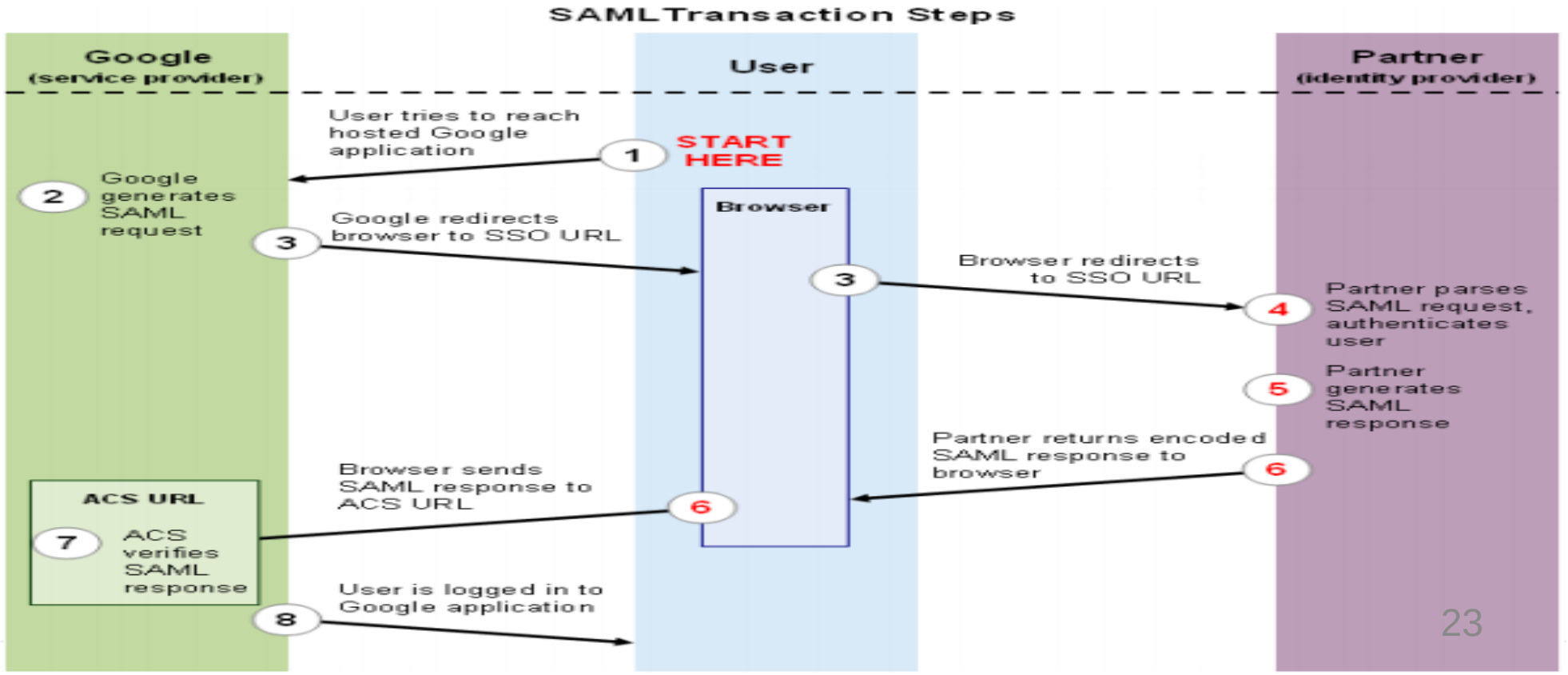
- Security Assertion Markup Language (SAML)
  - standard protocol for web browser single sign-on using secure tokens

Introduction to Security Assertion Markup Language (SAML)

https://www.youtube.com/watch?v=SSFuHtvkODo (6:13)

# SAML

- Security Assertion Markup Language (**SAML**)
  - doesn't rely on passwords, uses crypto and digital signatures to pass secure token from identity provider to application



# OAuth

- Open Authorization

  - open standard for token-based authentication and authorization on the Internet

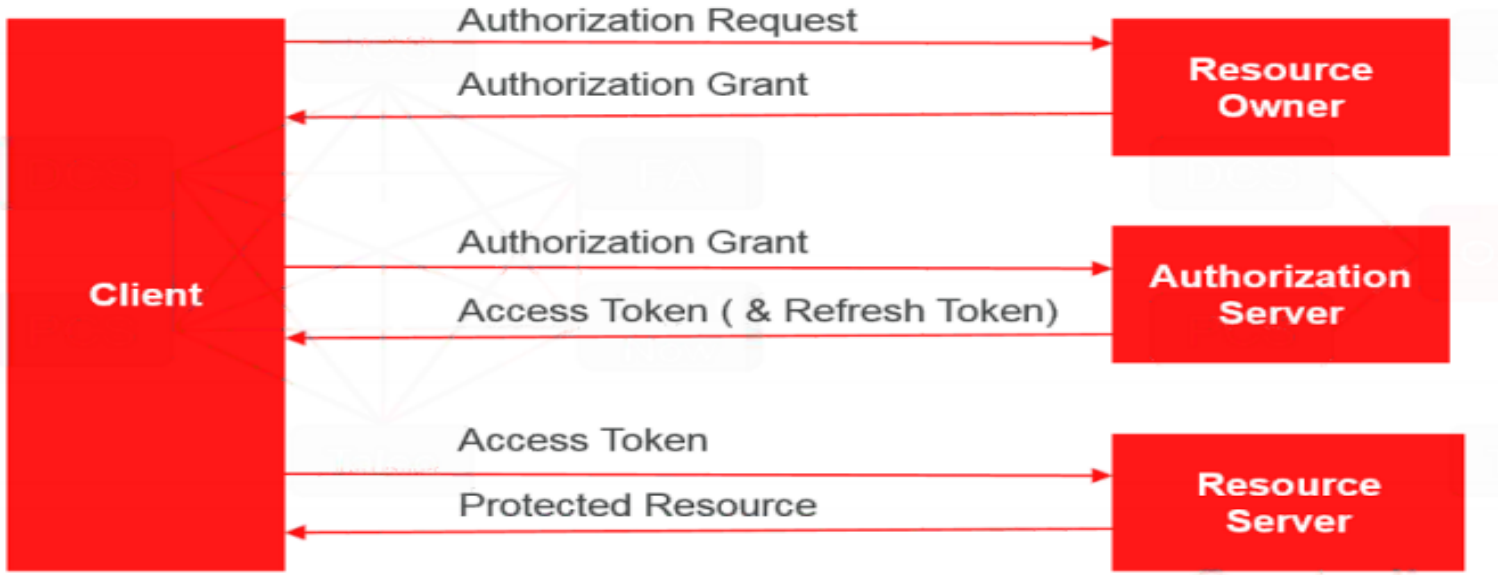
OAuth Introduction and Terminology

https://www.youtube.com/watch?v=zEysfgIbqlg (5:48)

University of Victoria

# OAuth

- Open Authorization (**OAuth**): open standard for token-based authentication and authorization; allows third party to use information without exposing password
  - just authorization to resources, not supposed to be authentication



# Identity - Summary

- prefer multifactor over single-factor
  - if single factor ensure long or strong
  - password complexity, expiration, recovery, lockout, history, reuse, length
- do not use generic or default accounts
  - change them if possible
- do not use shared accounts

University of Victoria

# Access Lifecycle

- **account management**: creating user accounts, modifying accounts, decommissioning accounts
  - **authentication**: verifying an identity (who they say they are)
  - **authorization**: verifying what someone is allowed to do
- **onboarding**: provide new employees the access they need
- **transfer**: adjusting access when changing roles
- **offboarding**: remove access from departing employees

# Logging

- record **who did what and when**
- different levels of logging maturity:
  - logs enabled
  - centralized logging
  - security information and event management (SIEM)
- ensure accurate time, synchronized
- restrict access, store remotely
- correlation, monitoring, alerting

"Superman" problem
- can't be in two places at once
- reference to SIEM use case that correlates logins from, for example, Vancouver and then also Paris

University of Victoria

not enough to just keep the logs, have to look at them

# Onboarding

- onboarding
  - provide access to new employees
    - delay impacts brand of company (desk, laptop, phone, access)
  - concept of an employee role or base role
    - that access that every employee has (eg. active directory)
  - “make me look like Bob”
    - leads to access creep
  - aggregation of privileges
    - longer an employee is there, the more access they have

# Onboarding

- employee badge
  - what should be on it?
  - company
  - department
  - name
  - employee number
  - signature
  - picture

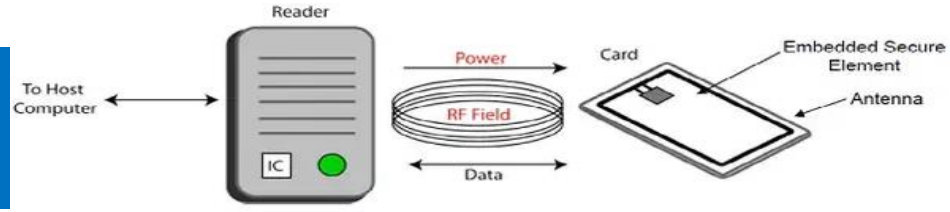

University of Victoria

# Cards

- what's inside it?
  - proximity card

    "dumb card"

  - smart card



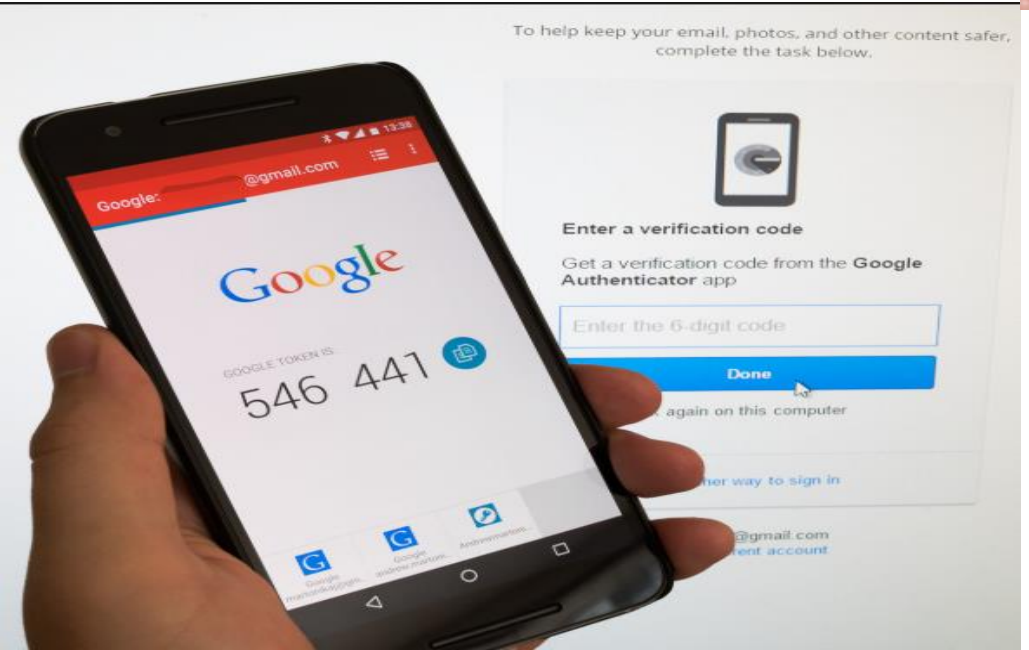



RFID sleeve


Faraday bag

University of Victoria

# Card Alternatives


# Useful tools

Handheld NFC Copier RFID Duplicator Ic Card Cloner Reader Writer with 125khz/250KHZ/375KHZ/500KHZ/13.56mhz

Brand: HACHANLUN

Price: CDN$ 18.58

Get a **$50 Amazon.ca Gift Card** instantly, plus up to 5% back for 6 months after approval for the Amazon.ca Rewards Mastercard.
Pay ~~$18.58~~ **$0.00** for this order after approval.

- ★ Card reading/writing function: Reading and writing can circulate more than 10 thousand times. Users can define access conditions and password by themselves. Widely used at community, school, office and other access control needed places.
- ★ Frequency can be automatically detected, and 125KHZ, 250KHZ, 375KHZ, 500KHZ, 13.56MHZ frequency is applicable.
- ★ Supports EM4305, EM5200, EM8800, T5577, ZX-F08 UID and supports ISO 14443 Type A and B.
- ★ Small size, conform to ergonomics, with built-in LED light and buzzer, convenient for carrying and daily usage. Clear function button design, makes it more simple to operate. Such a nice product, don't miss it!
- ★ We solemnly promise you that if you find problems with the product itself, you can contact us in time. we will definitely give you a reply in the first place and return it for you. please feel free to use it.

Report incorrect product information.


Click to open expanded view

English 10 Frequency NFC RFID Card Copier Writer Reader Duplicator for IC ID Cards,125kHz Cards,10pcs ID 125khz Cards + 10pcs ID 125kh Keyfobs + 10pcs 13.56mhz UID Key

Brand: SYWAN

★★★★☆ 96 ratings

Price: CDN$ 77.99

Get a **$50 Amazon.ca Gift Card** instantly, plus up to 5% back for 6 months after approval for the Amazon.ca Rewards Mastercard.
Pay ~~$77.99~~ **$27.99** for this order after approval.

New (2) from CDN$ 77.99 + FREE Shipping

- SUPPORT 10 FREQUENCY- ID-125KHz,ID-250KHz,ID-375KHz,ID-500KHz, ID-625KHz,ID-750KHz, ID-875KHz,ID-1000KHZ,IC-13.56MHZ,HID-125KHz
- COLOR SCREEN WITH VOICE DESIGN- 3.2inch HD color screen display, the RFID reader have voice operation promp
- CARD TYPE COMPATIBLE- Half-encrypted card compatible but not for fully-encrypted cards,can read EM4100, UID cards, T5577, EM4305 cards.not for hotel card,bank card and the card with balance
- NOTE- It doesn't work for fully-encrypted cards. By its decoding software, it may work for most half-encrypted cards, but not all.We hope you can confirm with us whether it can work for you through QA before purchasing.
- PACKAGE INCLUDE- 1 * Handheld RFID NFC Copier Reader Writer, 1 * USB cable, 10 * ID-125khz cards, 10 * IC-13.56mhz keyfobs ,10 * ID-125kh keyfobs

Report incorrect product information.

RFID Card Mini-Type Handheld 125 KHz Copier RFID Duplicator for All ID(EM4100) Cards, Cloner RFID Writer Chip Card Writer Clone RFID Card...

★★★★☆ 2

$27.49

Get it by **Tomorrow, Mar 13**

FREE Shipping on orders over $35 shipped by Amazon

Only 7 left in stock.

# Video

- Tap Fraud

https://www.youtube.com/watch?v=EKks3vfiy6Q (4:03)

Other:

https://www.youtube.com/watch?v=gJo9PfsplsY

https://www.youtube.com/watch?v=Y8mzyt8L_iY

https://www.youtube.com/watch?v=oT5yk959L7A

University of Victoria

5,326 views | Jan 30, 2017, 08:00am

## Hackers Lock Down Hotel Rooms In A New Twist On Ransom Attacks

Lee Mathews Contributor

Security

*Observing, pondering, and writing about tech. Generally in that order.*

When was the last time you used an actual key to unlock the door to your hotel room? It's been a long time. Computerized key card systems took over ages ago. They're mostly a tremendous convenience, both for guests and hoteliers -- that is, until someone hacks into the system that control the locks.

Image: Romantik Seehotel Jagerwirt

This just happened to a 111-year-old hotel in Austria. Management at the Romantik Seehotel Jaegerwirt told reporters that this was the third time they had been targeted by hackers. Once they had breached the key card system, guests were unable to enter their rooms and the front desk couldn't reprogram cards.

The hackers demanded that the hotel fork over €1500 (a little over $1,600, and payable in Bitcoin, naturally). Pay up, and control of the

# Offboarding

- offboarding
  - remove access from departing employees
  - remind about obligations regarding assets, info.
  - consider:
    - voluntary departure
      - competitor vs. not
      - exit interview
    - involuntary departure
      - policies (eg. straight to the door? respect)
      - priorities (eg. remote access first)
      - review last activities

# Offboarding

- some organizations will review the last activities of the employee

# Offboarding

- offboarding
  - physical concerns
    - collect badge, keys, computer, phone, credit card, USB, etc.
    - threat to employees?
    - tailgating


awareness
prevention
encrypted?
drives encrypted?


University of Victoria

# Single-Factor Authentication


- password length
  - eg. passphrase better than password (but MFA is better than both)

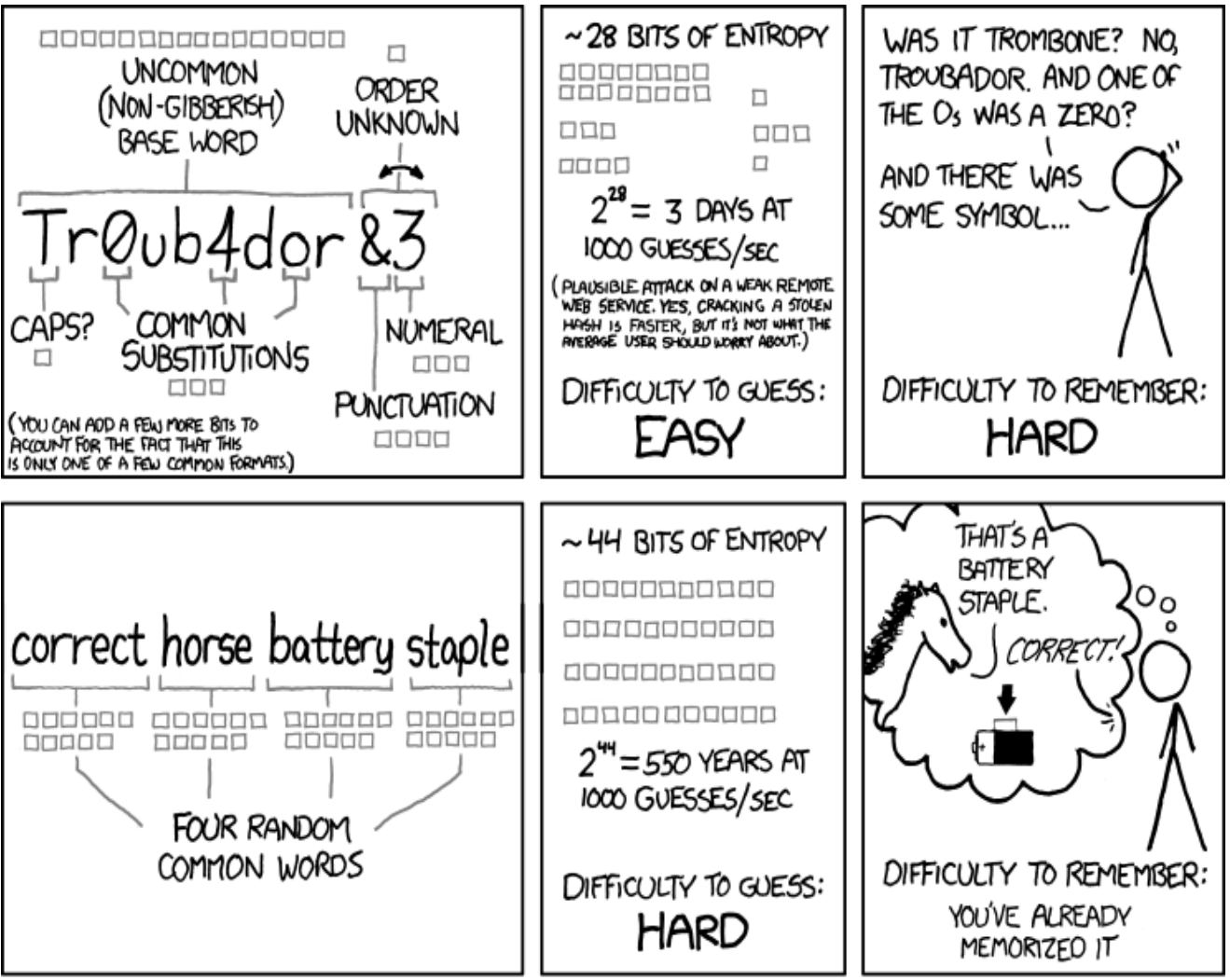
    eg. arepassphrasesbetterthanpasswords?
- password complexity
  - eg. upper, lowercase, punctuation

    Tr0ub4dor&3 ?
- password aging/expiry
  - eg. have to change password every 90 day
- password history
  - eg. system doesn't let you re-use any of last 5 passwords

    Summer2016
    Summer2017
    Summer2018
    Summer2019
    Summer2020

University of Victoria

# Passphrase




- use strong passwords
- don't share them with anyone
- include uppercase, lowercase, punctuation, a haiku and symbols
- make sure they are 20 characters long
- don't use the same one twice
- change them often
- don't write them down

NO!

https://xkcd.com/936/

# Single-Factor Authentication


- lockout after unsuccessful attempts
- determine whether to detect or prevent concurrent logins
- passwords are susceptible to attack
  - dictionary attack
  - brute force attack
  - rainbow tables

University of Victoria

# Hashing

- hashing (function converts one value to another)
- word -> hash
  - hello -> 5d41402abc4b2a76b9719d911017c592
- salt
  - QXLUPYFR
- hash
  - helloQXLUPYFR  6241a0505ef8c1a43b0f56e86a0e8886

can do an md5sum on text or a file (to know if you have the legitimate copy) – if the file changes so does the md5sum

```
$ echo -n "hello" | md5sum
5d41402abc4b2a76b9719d911017c592  -
$ echo -n "hello" | md5sum
5d41402abc4b2a76b9719d911017c592  -
$ echo -n "helloQXLUPYFR" | md5sum
6241a0505ef8c1a43b0f56e86a0e8886  -
$ echo -n "helloQXLUPYFR" | md5sum
6241a0505ef8c1a43b0f56e86a0e8886  -
```

```
$ md5sum passwd
ccbef84a758831685f9f4fb89382ebdf  passwd
$ md5sum passwd
ccbef84a758831685f9f4fb89382ebdf  passwd
$ echo " " >> passwd
$ md5sum passwd
77219932da9eb6dadbb92db63ddfee42  passwd
$ md5sum passwd
77219932da9eb6dadbb92db63ddfee42  passwd
```

University of Victoria

# Rainbow Tables

- example excerpt from a **rainbow table**
- holds a significant number of precomputed hashes
- can easily look up the hash and know what the original input was

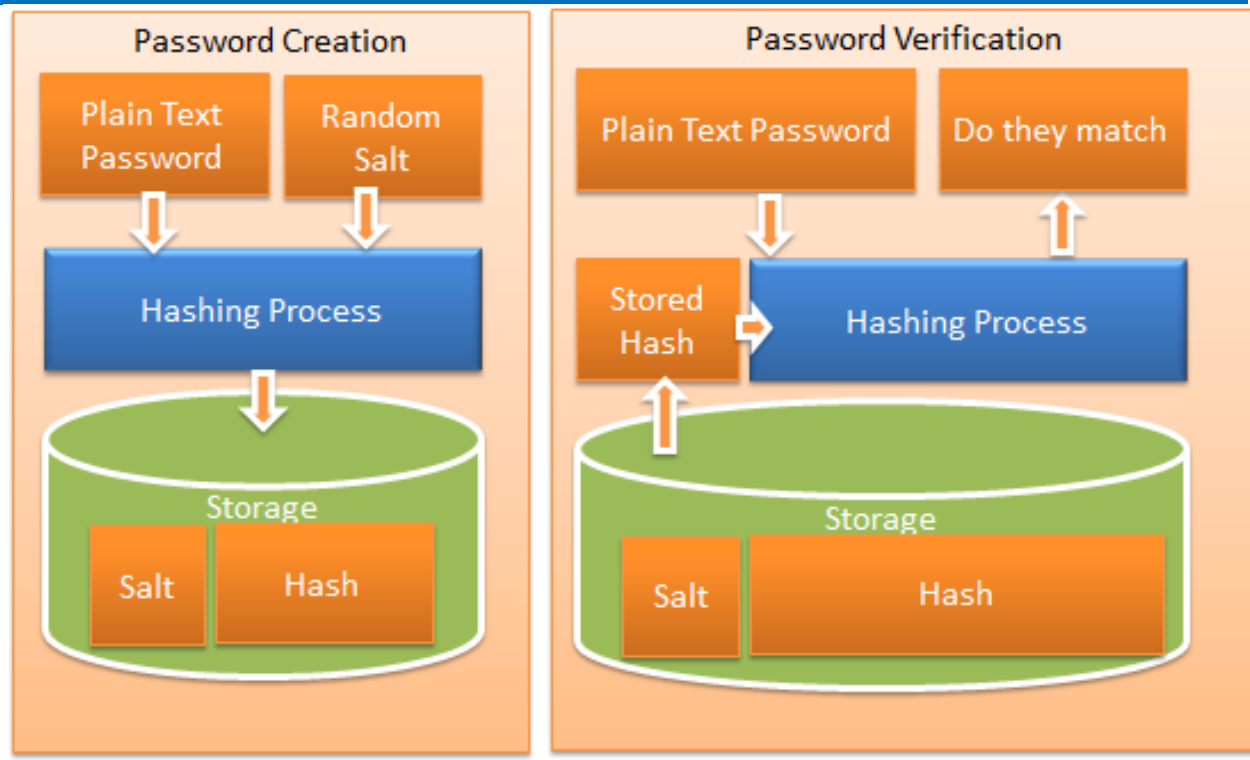
eg. 78df1f79d6f358e85e1b8e7c62b38a66

```
$ cat rain.txt
abc1111 78df1f79d6f358e85e1b8e7c62b38a66
abc1112 3823464a605526335f299ba168e341c6
abc1113 fcde8a9ad8769dbbaf8f5591b8cd17d9
abc1114 f15d0db7f664df4ff8b20640468cc233
abc1115 1f55800f1e1cd61ab9361c09f095eb1d
abc1116 7c8514556bde5d52715cf113a858654b
abc1117 d4568d336f015a6cf4672a0f666db5a9
abc1118 5dd9f42639957c5175bfdd727396fd2e
abc1119 bd9a20efe7dd54b677a202113d41cd1a
abc1120 8cb63301a2d64fa82941c788124800c1
abc1121 c02898fe2ed7f86e6dd6f7e9d5ee681b
abc1122 fdd4edc15214d2da945e021c5e8e1ed6
abc1123 fdc860609fd2d8c39ebbba81ab0b79e8
abc1124 62b41a971e0e621eeb73f540bb3d9d0b
abc1125 4e8025b01a798a359a153a3dc56be7fd
abc1126 9da51d3e4935dcf019fae38455d57ff9
abc1127 e0ffef9cb413dbc664ec3d9021761626
abc1128 10234f205efd94b6db58bf0a33f36928
abc1129 b001a776721001acf84411134e56e619
abc1130 a91afa66937386c358914e73fb06e207
abc1131 391f0ed54fa8d9038a60f83d13b2bb76
abc1132 6539b50a8d1630496b4d0e24c8374319
```

University of Victoria

# Salting the Hash

- password management
- password creation
- password = susceptible to rainbow tables
- password + salt -> hash = less susceptible to attacks
- … **unless the salt is short and have computed all combinations**




University of Victoria

# Information Security Policy

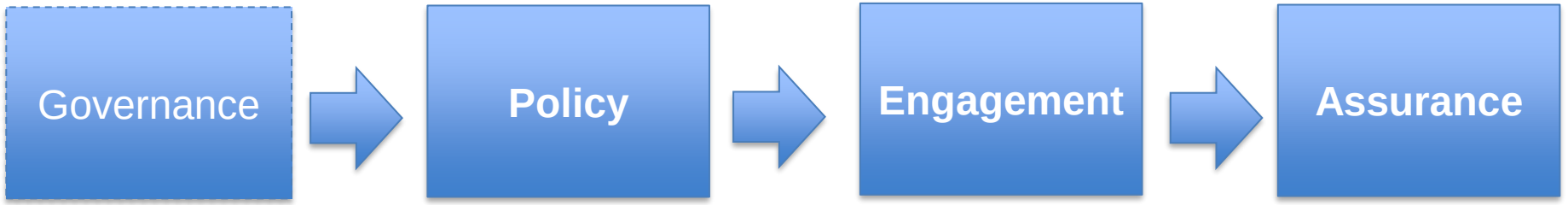
# Policies, Standards, and Guidelines

- **policy**: document that outlines requirements that must be met

  (eg. acceptable use policy)
- **standard**: system or procedure specific requirements that must be met

  (eg. server hardening, cryptographic)
- **guideline**:  collection of system or procedure specific “suggestions” for best practice
- policy should refer to standards and guidelines


# Information Security Policy




- vision
- mission
- goals
- strategy

- standards
- regulations
- laws

- education
- awareness
- training
- communications
- marketing

- compliance
- enforcement
- assurance

An information security policy is the cornerstone of an information security program. It should reflect the organization's objectives for security and the agreed upon management strategy for securing information.

Information Security Policy lets *parties* know what their responsibilities are, how to protect organization network/systems/data and lets them know what they may and may not do.

# Information Security Policy

BRITISH COLUMBIA

Menu

Home > British Columbians & Our Governments > Services & Policies for Government > Policies, Procedures & Standards >

- Appropriate Use Policy
- BCEA Policy & Procedure Manual
- Core Policy & Procedures Manual
- FOIPPA Policy & Procedures Manual
- **Information Security Policy**
- Intellectual Property Management
- Naming Privileges Policy
- IM/IT Standards
- Privacy Management & Accountability Policy
- Purchase Card Manual
- Recorded Information Management Manual
- Web Content & Development Guides
- Working Outside the Workplace Policy
- Mobile Device Guidelines

## Information Security Policy


**INFORMATION SECURITY POLICY V4.0 HAS ARRIVED!**

The Government of British Columbia is committed to providing services to citizens that are efficient and secure. Through the adoption of new technologies, the government seeks to provide improved services while maintaining the security of government information assets.

### About the Information Security Policy (ISP)

**The Information Security Policy V4.0 (PDF) has been updated, it is now:**

- Easier for users to understand
- Structured so that key information is easy to find
- Shorter and more accessible.

The ISP 4.0 (PDF) provides the foundation for the information security governance program, which includes standards, procedures, training and awareness material, all of which are used to protect government information and information systems

**'Security is everyone's responsibility'**

All employees need to be aware of their responsibilities to safeguard government information. The Information Security Policy supports security requirements in the *Freedom of Information and Protection of Privacy Act* and the *Information Management Act*.

Supplemental to the B.C. government Core Policy and Procedures Manual and the Appropriate Use Policy, this policy provides the framework for government organizations to establish local policies and procedures necessary for the protection of information and technology assets for the Province of British Columbia.

### Additional Resources

- Information Security Policy (PDF)
- Core Policy and Procedures Manual
- Appropriate Use Policy
- Information Incident Management Process
- IM/IT Standards

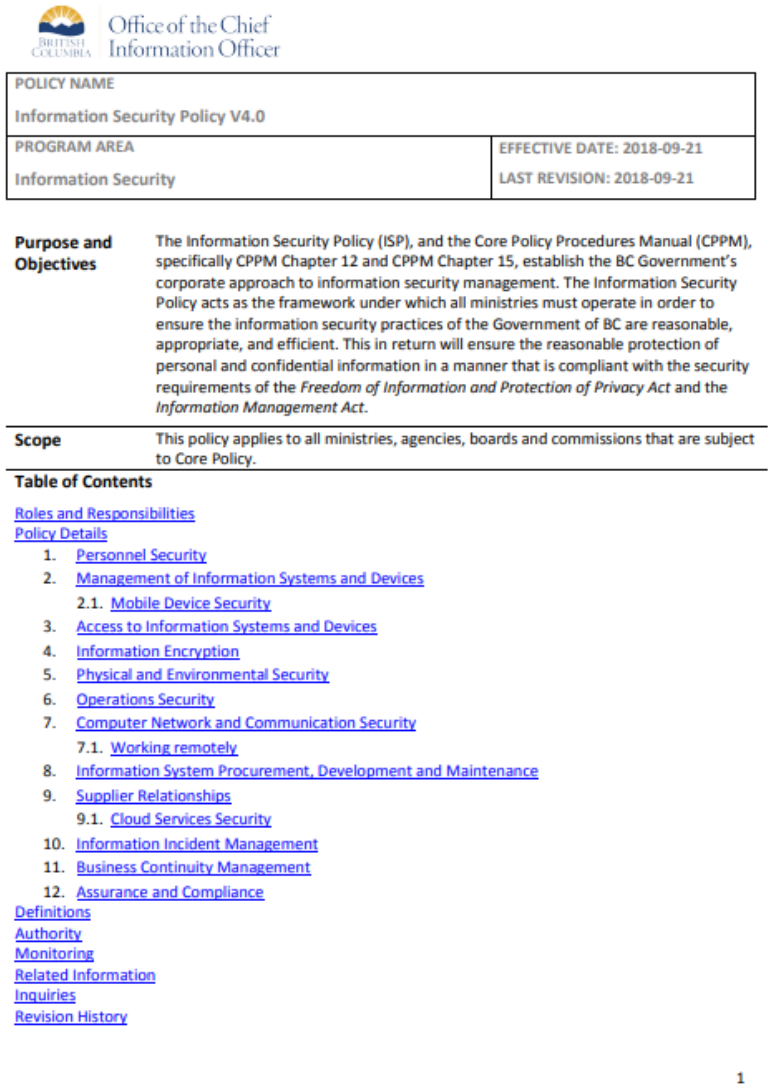
### Contact Information

For additional information, please contact us.

# Information Security Policy

- do people know it exists? where is it?
- are they required to read it? can they understand it?
- how long is it? is the language at the right level?
- who does it apply to?
- is it followed? are there any “teeth” or penalties for not following?
- is it reviewed, updated, relevant?

# Information Security Policy



Office of the Chief Information Officer

| POLICY NAME | |
|---|---|
| Information Security Policy V4.0 | |
| PROGRAM AREA | EFFECTIVE DATE: 2018-09-21 |
| Information Security | LAST REVISION: 2018-09-21 |

**Purpose and Objectives** The Information Security Policy (ISP), and the Core Policy Procedures Manual (CPPM), specifically CPPM Chapter 12 and CPPM Chapter 15, establish the BC Government's corporate approach to information security management. The Information Security Policy acts as the framework under which all ministries must operate in order to ensure the information security practices of the Government of BC are reasonable, appropriate, and efficient. This in return will ensure the reasonable protection of personal and confidential information in a manner that is compliant with the security requirements of the *Freedom of Information and Protection of Privacy Act* and the *Information Management Act*.

**Scope** This policy applies to all ministries, agencies, boards and commissions that are subject to Core Policy.

**Table of Contents**



1

- policy language
- know the audience
- length
- clarity
- consumable
- base on an industry standard… why?

# Personnel Security

**Personnel Security**

This section identifies security responsibilities and management processes throughout the employment cycle.

Supervisors must ensure:

(a) Prior to employment, employee security screening is done in accordance with Public Service Agency policies and practices;

(b) During employment, employees are informed about the information security policies and procedures, Information Security roles and responsibilities;

(c) At termination, employees are reminded of their ongoing confidentiality responsibilities following termination of employment in accordance with the Standards of Conduct;

(d) Potential or actual information security breaches are investigated and reported, and invoke incident management processes where necessary; and

(e) Contractor responsibilities for information security are identified in contractual agreements.

# Information Systems and Devices

**Management of Information Systems and Devices**

This section defines requirements for secure management of government information systems and devices.

Ministries must:

(a) Maintain an inventory of government information systems and devices, including portable storage devices, and mobile devices;

(b) Validate the measures taken to protect information systems and devices as part of an enterprise risk management strategy. This includes maintaining, documenting, verifying and valuing asset inventories on a regular basis;

(c) Document the return of government devices in the possession of employees upon termination of their employment;

(d) Remove government information from devices that are no longer needed by government; and

(e) Securely dispose of devices in a manner appropriate for the sensitivity of the information the device contained.

**Mobile Device Security**

Ministries must ensure controls are implemented to mitigate security risks associated with the use of mobile devices.

Mobile device users must lock and/or secure unattended mobile devices to prevent unauthorized use or theft.

# Access to Info Systems and Devices

**Access to Information Systems and Devices**

This section identifies security roles, responsibilities and management processes relating to access and authorization controls for government information systems and devices.

Ministries must define, document, implement, communicate and maintain procedures to ensure access to government information systems and devices are granted to individuals based on business requirements and the principles of “least privilege” and “need-to-know.”

Supervisors must:

(a) Ensure the assignment and revocation of access rights follow a formal and documented process;

(b) Regularly, and upon change of employment, review, and update where appropriate, employee access rights to ensure they are up to date.

Employees must know and adhere to password security practices given in the Appropriate Use Policy.

University of Victoria

# Information Encryption

**Information Encryption**

This section defines encryption methods for improving the protection of information and for reducing the likelihood of compromised sensitive information.

The Office of the Chief Information Officer must:

(a) Provide direction and leadership in the use of encryption and the provision of encryption services, including those used for user registration; and

(b) Set corporate direction for the management (generating, storing, archiving, distributing, retiring and destroying) of encryption keys throughout their lifecycle.

The Chief Information Security Officer supports, and provides advice on, the use of encryption technologies in government.

Ministries must:

(a) Select information encryption controls during system design to provide appropriate protection commensurate to the information value and security classification; and

(b) Register the use of encryption technology products and services with the Chief Information Security Officer.

# Physical Security

**Physical and Environmental Security**

This section identifies operational requirements for protecting facilities where government information and information systems are located.

Ministries in collaboration with the Ministry of Citizens' Services, must:

(a) Design, document and implement security controls for a facility based on an assessment of security risks to the facility;

(b) Review, and where appropriate test, physical security and environmental control requirements;

(c) Establish appropriate entry controls to restrict access to secure areas, and to prevent unauthorized physical access to government information and devices;

(d) Incorporate physical security controls to protect against natural disasters, malicious attacks or accidents; and

(e) Ensure security controls are maintained when computer equipment, information or software is used outside government facilities.

# Operations Security

**Operations Security**

This section establishes a framework for identifying requirements to control, monitor, and manage information security changes to the delivery of government services.

Ministries must:

(a) Plan, document and implement change management processes to ensure changes to information systems and information processing facilities are applied correctly and do not compromise the security of information and information systems;

(b) Monitor and maintain information systems software throughout the software lifecycle;

(c) Define, document, assess, and test backup and recovery processes regularly;

(d) Implement processes for monitoring, reporting, logging, analyzing and correcting errors or failures in information systems reported by users and detection systems;

(e) Ensure operating procedures and responsibilities for managing information systems and information processing facilities are authorized, documented and reviewed on a regular basis;

(f) Establish controls to protect log files from unauthorized modification, access or disposal;

(g) Establish processes to identify, assess, and respond to vulnerabilities; and

(h) Enable synchronization of computer clocks to ensure integrity of information system logs and accurate reporting.

The Chief Information Security Officer must assess, provide advice, monitor response progress, and report on vulnerability response activities.


# Computer Network and Communication Security

**Computer Network and Communication Security**

This section identifies requirements for the protection of sensitive or confidential information on computer networks.

The Government Chief Information Officer must provide direction and leadership on implementation of, and significant modification to, electronic messaging systems.

The Chief Information Security Officer must develop corporate security controls to protect information from interception, copying, misrouting and unauthorized disposal when being transmitted electronically.

Ministries in collaboration with the Office of the Chief Information Officer must:

(a) Document network security controls prior to commencement of service delivery;

(b) Ensure security features are implemented prior to commencement of service delivery;

(c) Document, implement and manage changes to network security controls and security management practices to protect government information systems from security threats;

(d) Ensure segregation of services, information systems, and users to support business requirements based on the principles of least privilege, management of risk and segregation of duties;

(e) Ensure implementation of network controls to prevent unauthorized access or bypassing of security control;

(f) Ensure electronic messaging services are protected commensurate to the value and sensitivity of message content, and approved for use by the Government Chief Information Officer.; and

(g) Ensure information transfers between government and external parties are protected using services approved for use by the Government Chief Information Officer.

# Information System Procurement, Development and Maintenance

**Information System Procurement, Development and Maintenance**

This section defines requirements to ensure security controls are included in business and contract requirements for building and operating secure information systems, including commercial off the shelf and custom-built software.

Ministries must:

(a) Develop, implement and manage the processes and procedures necessary to ensure that information security risks and privacy requirements are taken into account throughout the systems development lifecycle;

(b) Ensure sufficient resources and funding are allocated to complete the necessary information security tasks;

(c) Ensure that system development or acquisition activities are aligned with government information security requirements and standards;

(d) Apply vulnerability scanning, security testing, and system acceptance processes commensurate to the value and sensitivity of the information system.

The Office of the Chief Information Officer must provide corporate direction and oversight for developing and implementing security standards to procure, develop and maintain information systems.

# Supplier Relationships

**Supplier Relationships**

This section defines requirements to ensure supplier agreements for information systems and cloud services align with government security policies, standards and processes.

Ministries must:

(a) Ensure identified security requirements are agreed upon and documented prior to granting external parties access to information, information systems or information processing facilities;

(b) Ensure security controls, service definitions, and delivery levels are identified and included in agreements with external parties prior to using external information and technology services;

(c) Establish processes to manage and review the information security controls of services delivered by external parties, on a regular basis;

(d) Ensure that changes to the provision of services by suppliers of information system services take into account the criticality of the information and information systems involved and the assessment of risks;

(e) Assess business requirements and associated risks related to external party access to information and information systems; and

(f) Ensure the risks of external party access to information and information systems are identified, assessed, mitigated and managed.

# Cloud Services Security

**Cloud Services Security**

The Office of the Chief Information Officer provides corporate direction and leadership on the secure use of cloud services by:

(a) Establishing policy and providing strategic direction on the use of cloud services;

(b) Establishing roles and responsibilities;

(c) Establishing information security requirements for cloud services.

Ministries must:

(a) Notify the Government Chief Information Officer and the Chief Records Officer prior to procuring cloud services; and

(b) Consider existing cloud service offerings provided by the Office of the Chief Information Officer prior to procuring new cloud services.

(c) Ensure new cloud services align with the cloud service strategy provided by the Office of the Chief Information Officer.

# Supplier Relationships

**Information Incident Management**

This section addresses the response and management of information incidents, including privacy breaches, in order to take the appropriate steps to mitigate the risk of harm.

Employees must immediately report suspected or actual information incidents in accordance with the Information Incident Management Process.

Ministries must establish ministry specific information incident management policies and procedures, as appropriate, to ensure quick, effective and orderly response to information incidents within the ministry.

**Business Continuity Management**

This section defines requirements to prepare, and re-establish, business or services as swiftly and smoothly as possible in adverse situations.

Emergency Management BC coordinates government-wide business continuity plans to reconcile recovery priorities, business impacts, security impacts and business resumption processes.

Ministries must:

(a) Establish, document, implement, and maintain processes, procedures and controls to ensure the required level of information security for business continuity and disaster recovery during an adverse situation;

(b) Ensure that vital records and critical systems are identified in business continuity plans;

(c) Review business continuity and recovery plans annually to ensure they are current, valid, functional and readily accessible during a business interruption; and

(d) Regularly conduct business continuity and recovery exercises and, where necessary, update business continuity and recovery plans.

# Assurance and Compliance

**Assurance and Compliance**

This section defines requirements to ensure compliance with legislation, government policies and standards.

The Chief Information Security Officer must:

(a) Initiate an independent review of the overall government information security program on a regular basis; and

(b) In collaboration with ministries, report on each ministry's adherence to the information security policies, and standards.

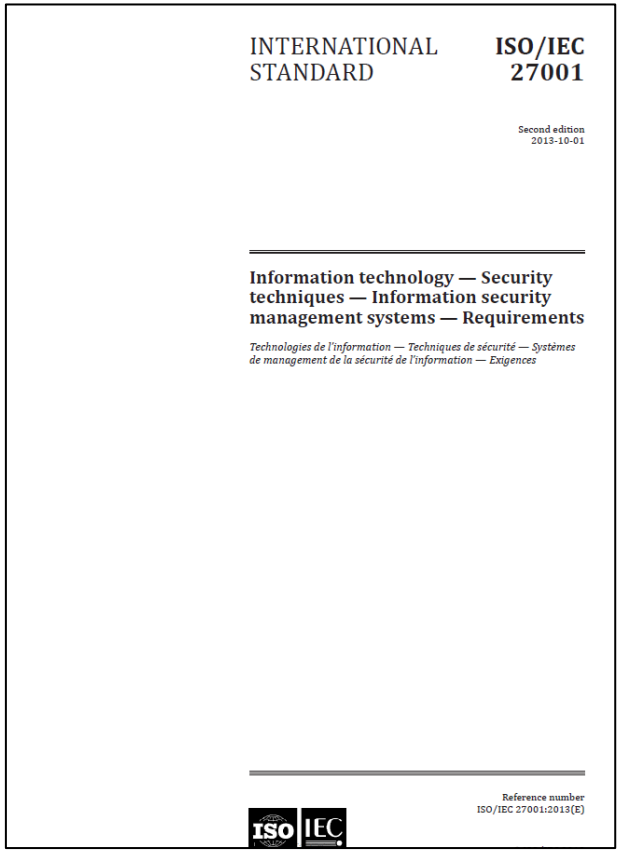
Ministries must:

(a) Ensure the legislative, statutory, regulatory and contractual security requirements of information systems are identified, documented, addressed and maintained; and

(b) Regularly review information systems and information security procedures to ensure compliance with security policies and standards.

# Information Security Standards

# ISO/IEC 27001



INTERNATIONAL STANDARD

**ISO/IEC 27001**

Second edition
2013-10-01

**Information technology — Security techniques — Information security management systems — Requirements**

*Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*

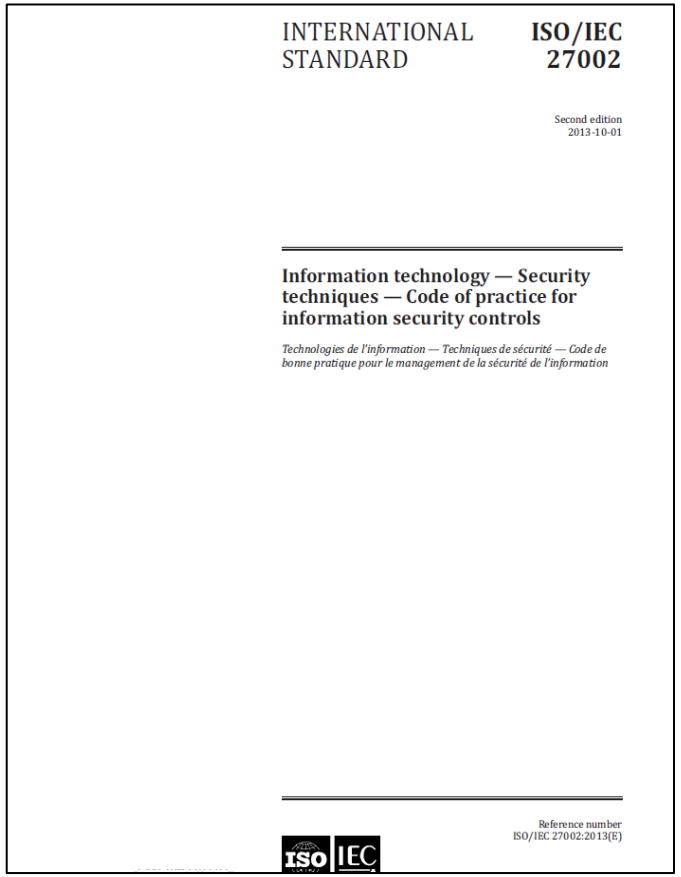
Reference number
ISO/IEC 27001:2013(E)

ISO IEC

University of Victoria

## Contents

# ISO/IEC 27002


INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2013-10-01

Information technology — Security techniques — Code of practice for information security controls

*Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*

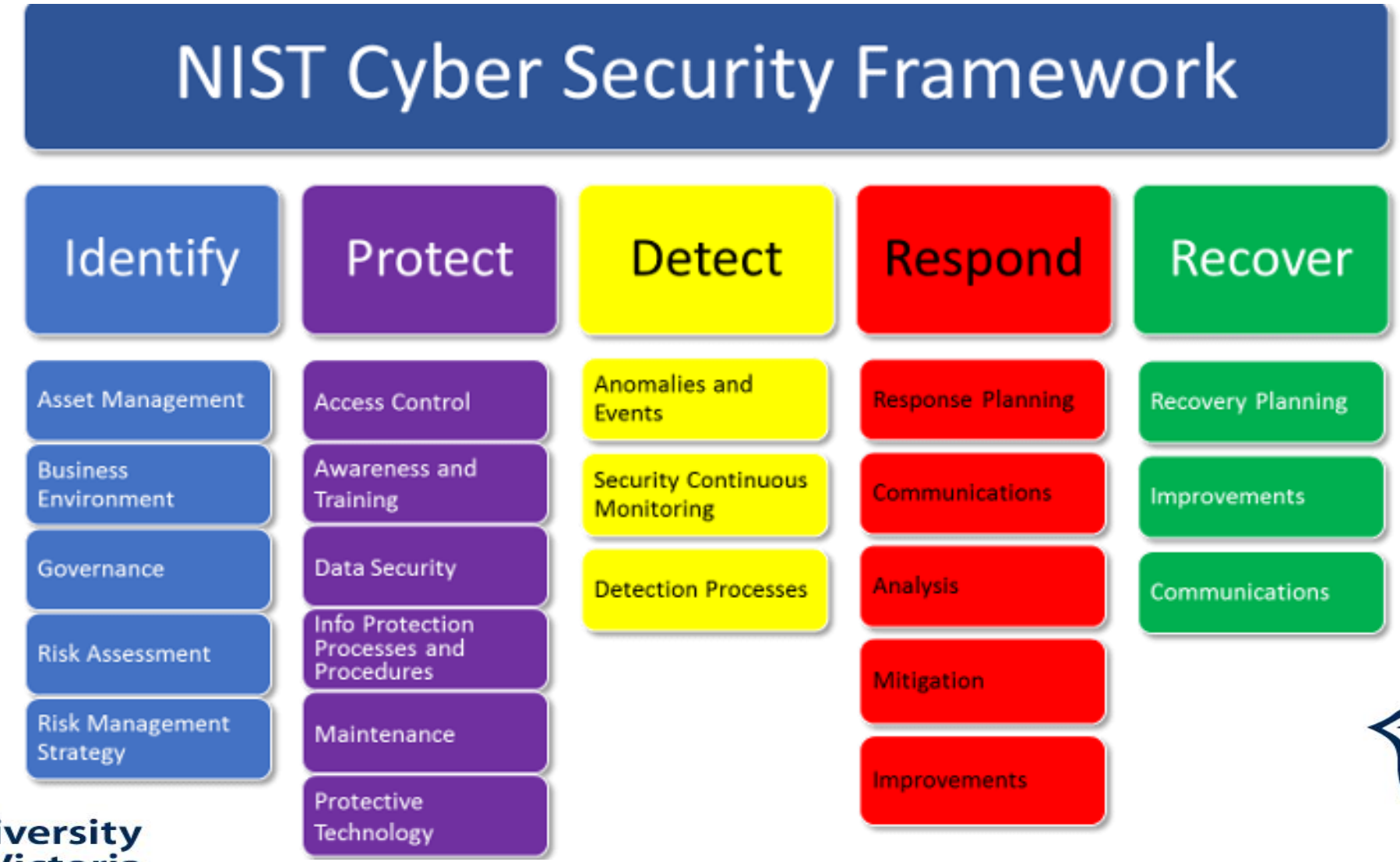
Reference number
ISO/IEC 27002:2013(E)

ISO IEC

University of Victoria

## Contents

# NIST




University of Victoria

https://securityaffairs.co/wordpress/58163/laws-and-regulations/nist-cybersecurity-framework-2.html

# NIST

| | |
|---|---|
| **IDENTIFY (ID)** | **Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.** |
| | **Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.** |
| | **Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.** |
| | **Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.** |
| | **Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.** |
| **PROTECT (PR)** | **Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.** |
| | **Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.** |
| | **Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.** |
| | **Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.** |
| | **Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.** |
| | **Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.** |

# NIST

| | |
|---|---|
| **DETECT (DE)** | **Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.** |
| | **Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.** |
| | **Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.** |
| **RESPOND (RS)** | **Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.** |
| | **Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.** |
| | **Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.** |
| | **Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.** |
| | **Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.** |
| **RECOVER (RC)** | **Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.** |
| | **Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.** |
| | **Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.** |

# Audits

# Sarbanes Oxley / SOX

**SOX Section 404: Establish Controls to Support Accurate Financial Reporting**
According to SOX, all businesses should have internal controls in place for accurate and transparent financial reporting. An external auditor should review these controls every year, assessing how well businesses document, test, and maintain those internal controls.
The IT team's role here is to identify key IT systems and processes involved in initiating, authorizing, processing and summarizing financial information. This material usually involves security, application testing, the verification of software integrations, and automated process testing. The goal is to ensure all procedures support the accurate and complete transmission of financial data while keeping asset-bearing accounts secure from unauthorized access.

- access (physical and logical)
- incident / change management – show evidence of incident and change
- backup procedures



https://blog.ipswitch.com/sox-compliance-what-is-the-it-teams-role

# SAS70 / SSAE16 / SSAE18

- can help with SOX compliance
- SOC = Service Organization Controls
- three SOC reports:
  - SOC 1: financial statement controls
  - SOC 2: security; includes auditor testing and results
  - SOC 3: less detailed, intended to be publicly available
- two types:
  - Type 1: controls are suitably designed
  - Type 2: controls are suitably designed and operating effectively

# PCI - DSS (much more stringent)

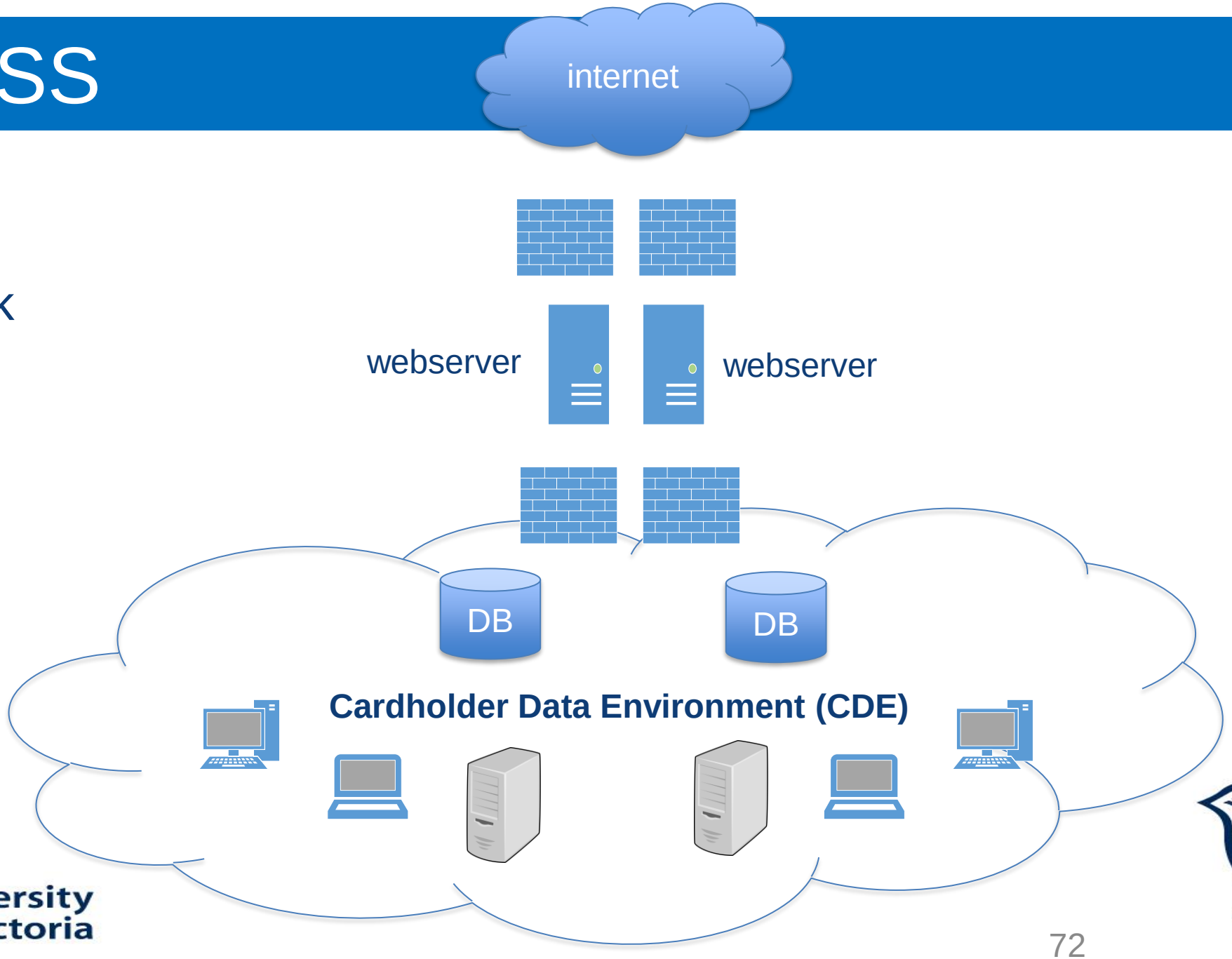
- focused on credit cards
- avoid if possible
- outsource if possible
- if must be involved then reduce Cardholder Data Environment (CDE) as much as possible
- reduce scope (eg. WiFi, rest of network)

| Goals | PCI DSS Requirements |
|---|---|
| Build and Maintain a Secure Network and Systems | 1. Install and maintain a firewall configuration to protect cardholder data<br>2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data | 3. Protect stored cardholder data<br>4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | 5. Protect all systems against malware and regularly update anti-virus software or programs<br>6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 7. Restrict access to cardholder data by business need to know<br>8. Identify and authenticate access to system components<br>9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data<br>11. Regularly test security systems and processes |
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security for all personnel |

pcisecuritystandards.org

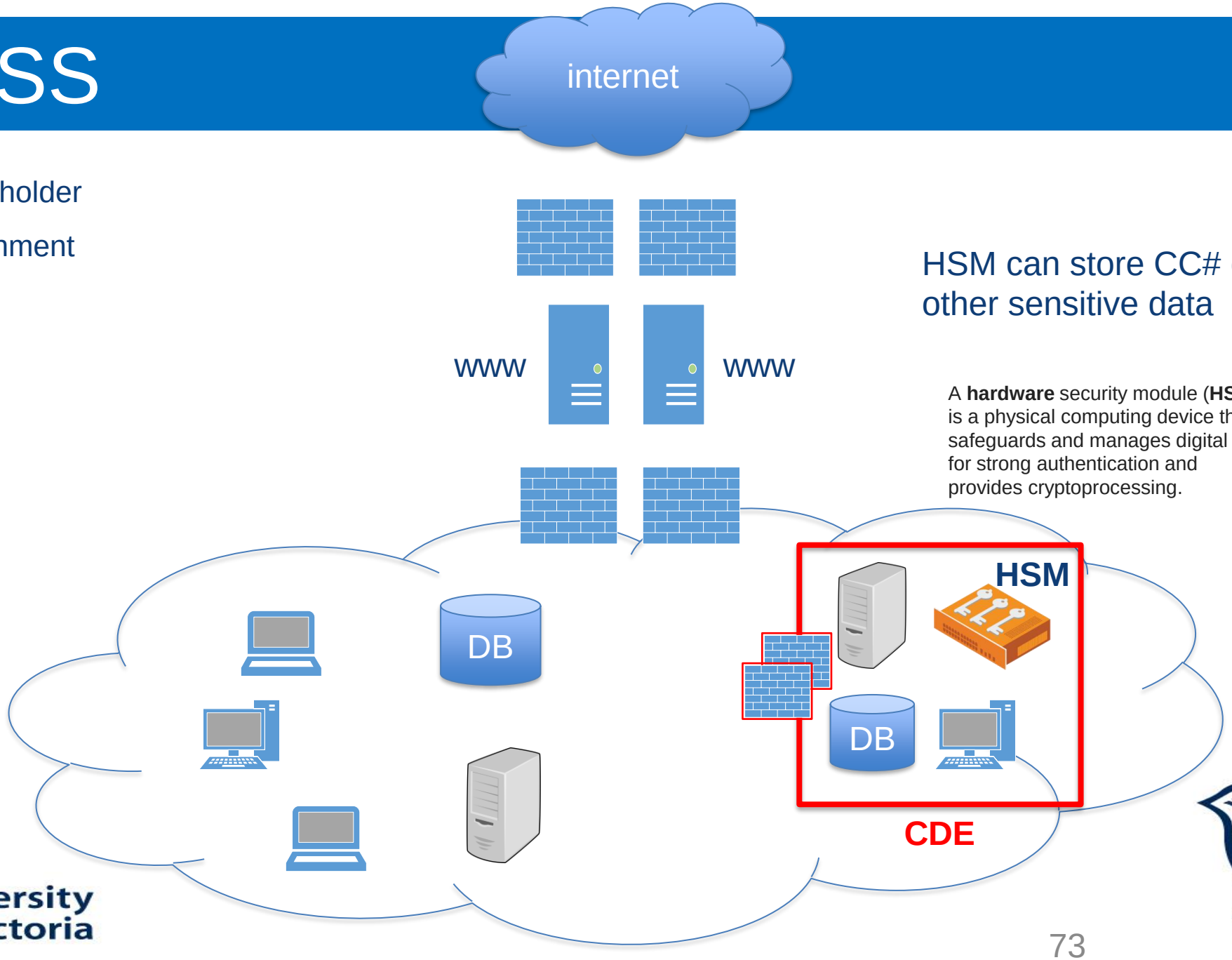
# PCI - DSS

- sample network



# PCI - DSS

- CDE = cardholder data environment

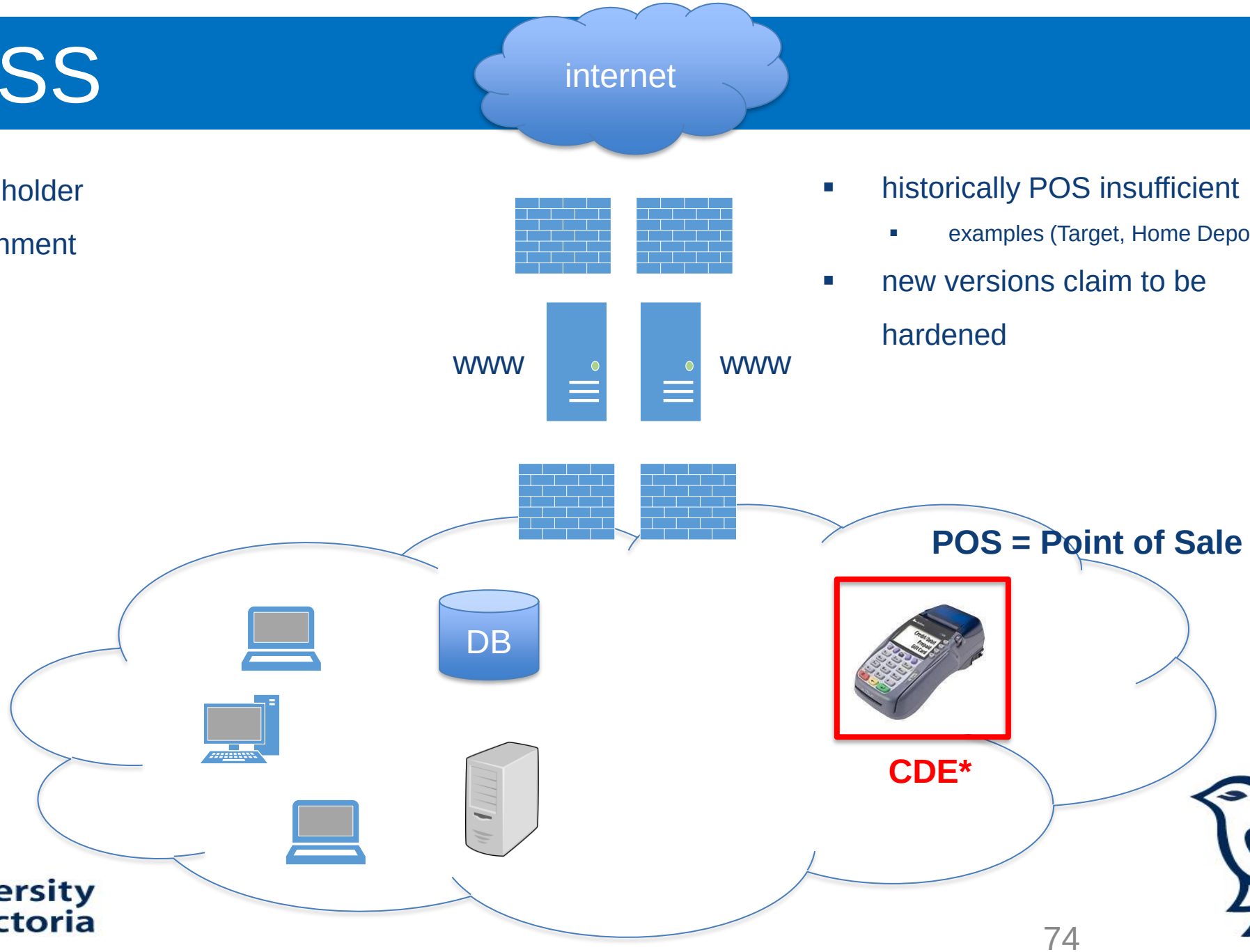



HSM can store CC# or other sensitive data

A **hardware** security module (**HSM**) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.

# PCI - DSS

- CDE = cardholder data environment




- historically POS insufficient
  - examples (Target, Home Depot)
- new versions claim to be hardened

University of Victoria

# Assigned Reading

- read Chapters 15-19 for next time

- lab is optional (NMAP)


University
of Victoria