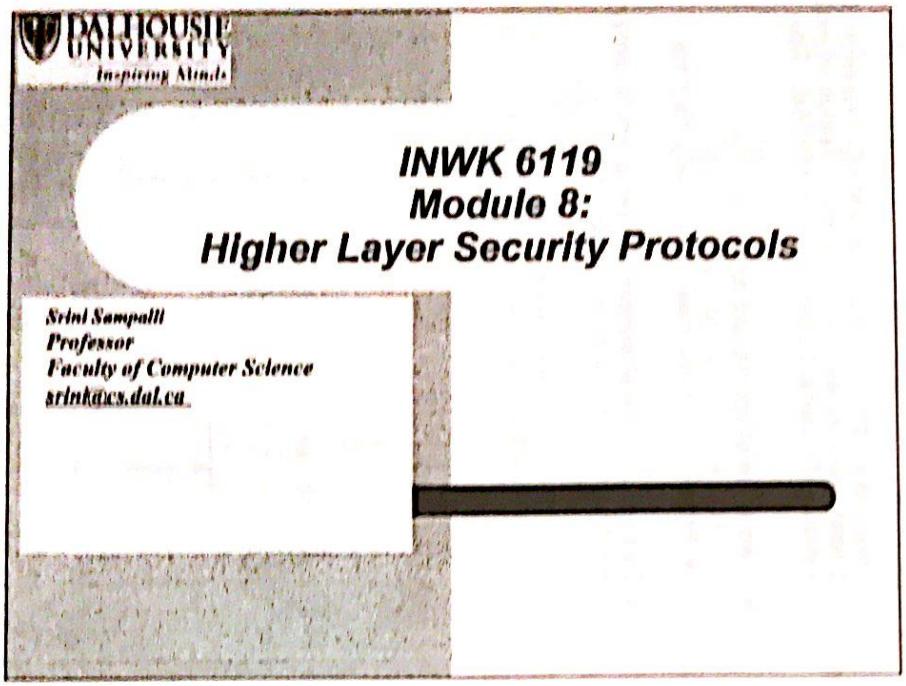
PARAS H. DUDHATRA B00728686.




- Pretty Good Privacy (PGP)
  - Email
  - File Storage Applications
- Secure Electronic Transaction (SET)
  - ECommerce Security

## *Pretty Good Privacy (PGP)*

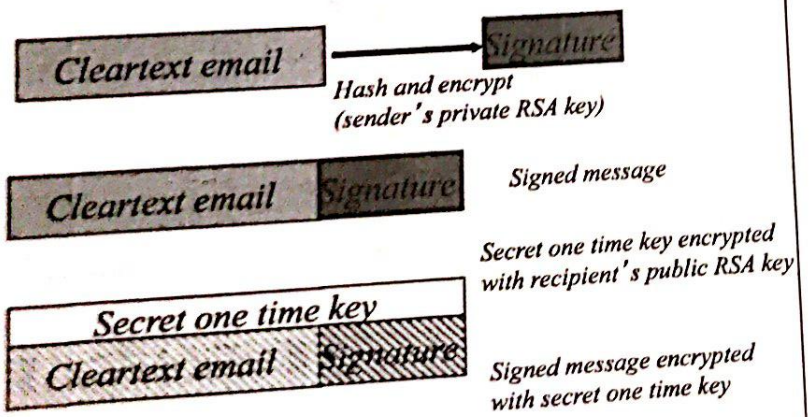
*"If privacy is outlawed, only outlaws will have privacy"*
*– Phil Zimmermann*

- ***Security service for email and file storage applications.***
- **Largely the effort of Phil Zimmermann (www.philzimmermann.com), who proposed and implemented the system.**
- **PGP is available both as a freeware and commercial software (Visit the International PGP home page – http://www.pgpi.org)**
- **Another excellent reference for configuring PGP is at www.emailprivacy.info/privacy_pgp**

## *PGP Basics*

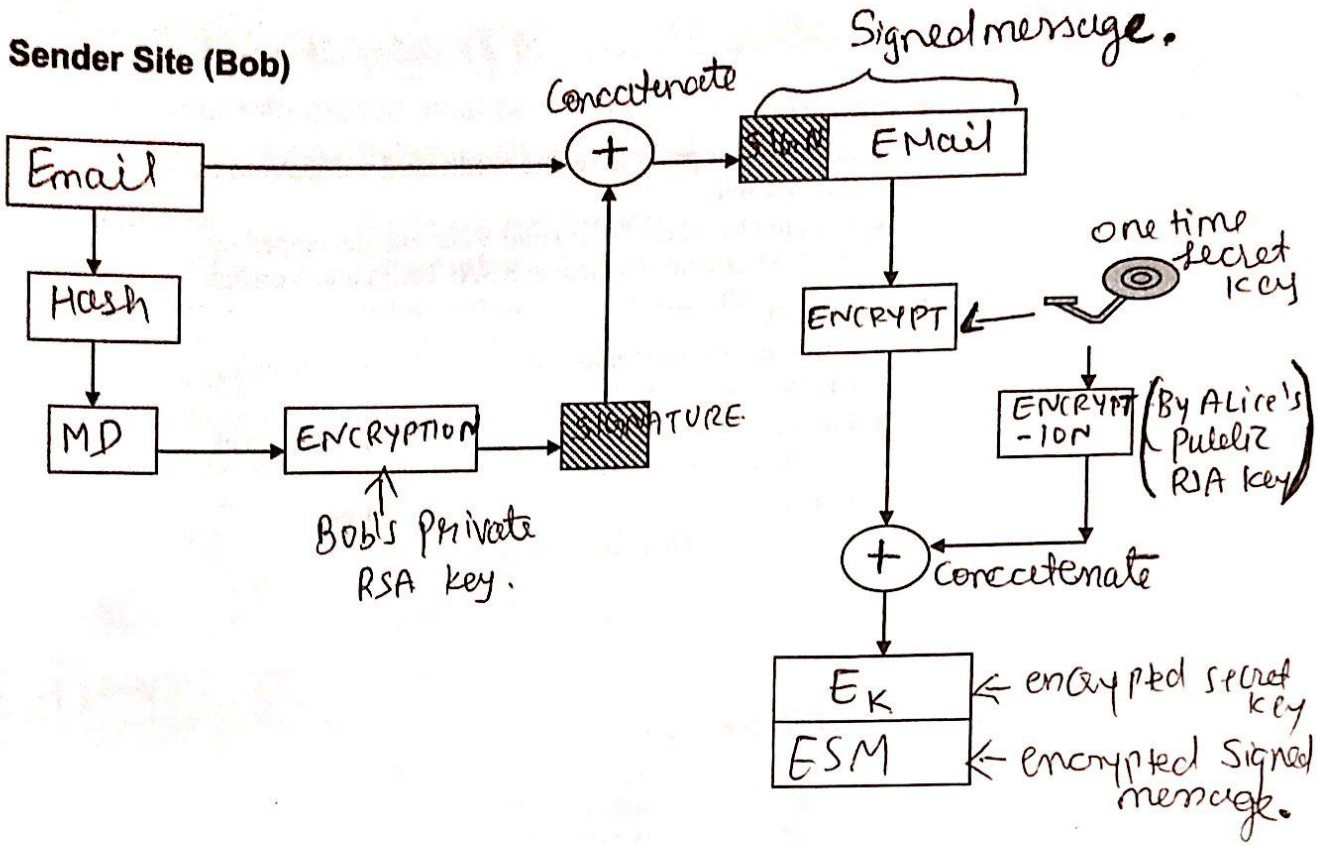
- **Provides confidentiality, integrity, authentication and non-repudiation for email and files.**
- **Runs on a variety of platforms (MAC, Windows, Unix, Linux) and can be integrated into a variety of mail systems (Outlook, Eudora, Claris, MHMail, Pine, etc.)**
- **Two types of encryption are used:**
  - **Public Key Cryptosystem – RSA**
  - **Private Key Cryptosystem – 3DES, IDEA, CAST128**
- ***Each time an email message is sent, a new secret key is randomly generated at the sender site.***

## *PGP Basics (cont'd.)*

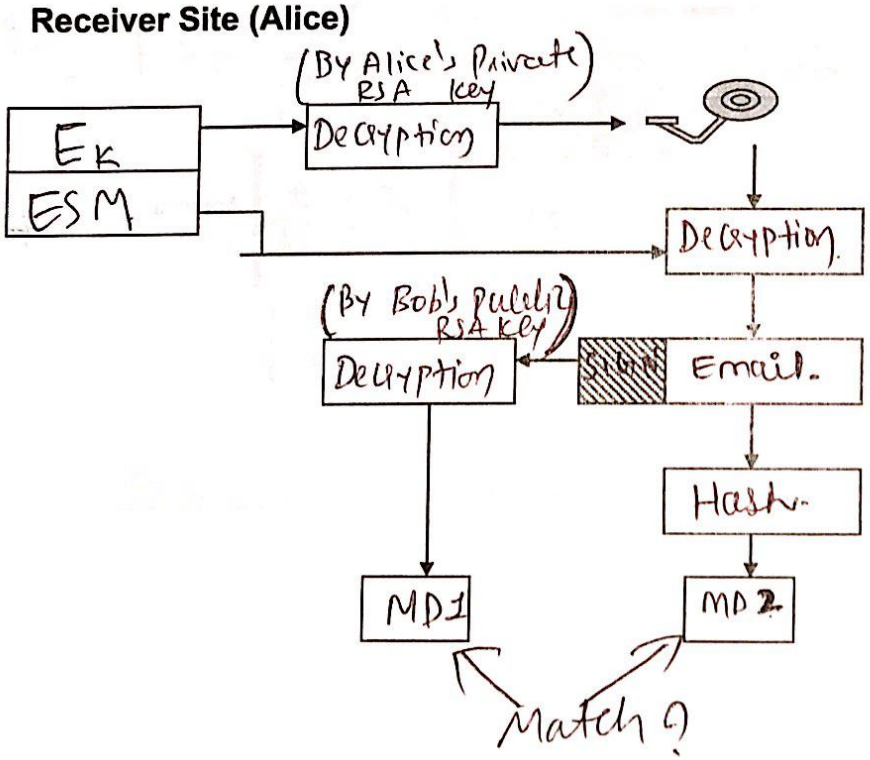


## PGP OPERATION

**Sender Site (Bob)**



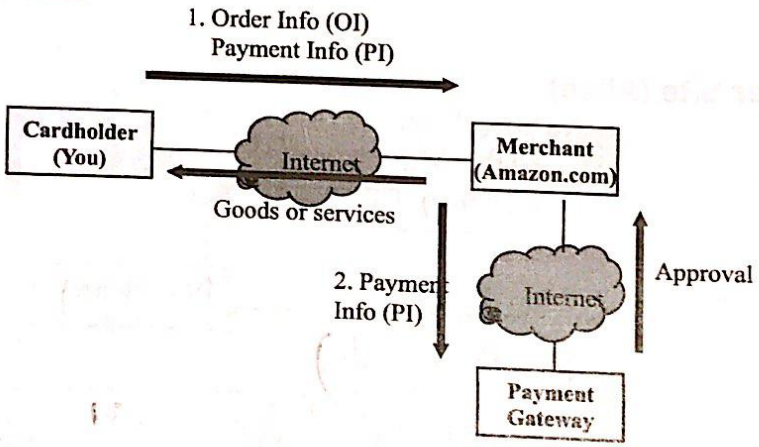

**Receiver Site (Alice)**



# Secure Electronic Transaction (SET)

- ***Overview***
  - Designed to provide secure credit card transactions over the Internet.
  - Initiated by Master Card and Visa, and developed by IBM, Microsoft, Netscape, RSA, Terisa and Verisign.
- ***Features***
  - Provides confidentiality of cardholder account and payment information.
  - Provides integrity of the order information, personal information and payment instructions.
  - Provides cardholder account authentication.
  - Provides merchant authentication.

# *SET Process*

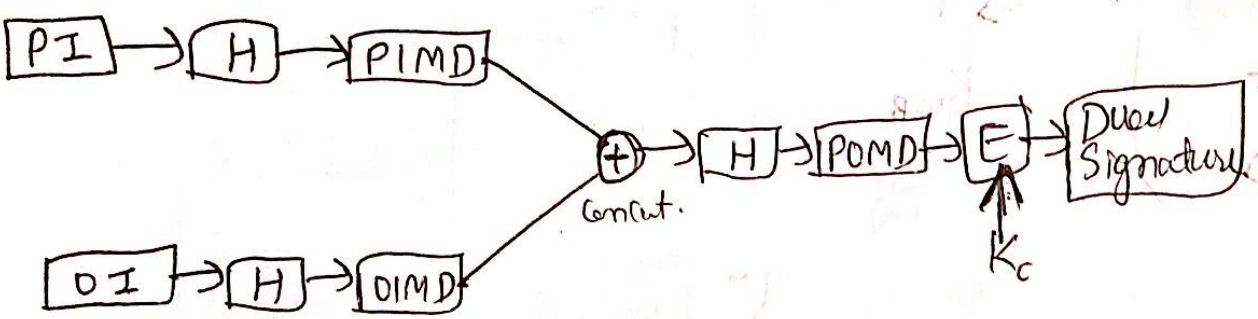


## Dual Signature

Purpose of dual signature is to link two messages that are intended for two different recipients:

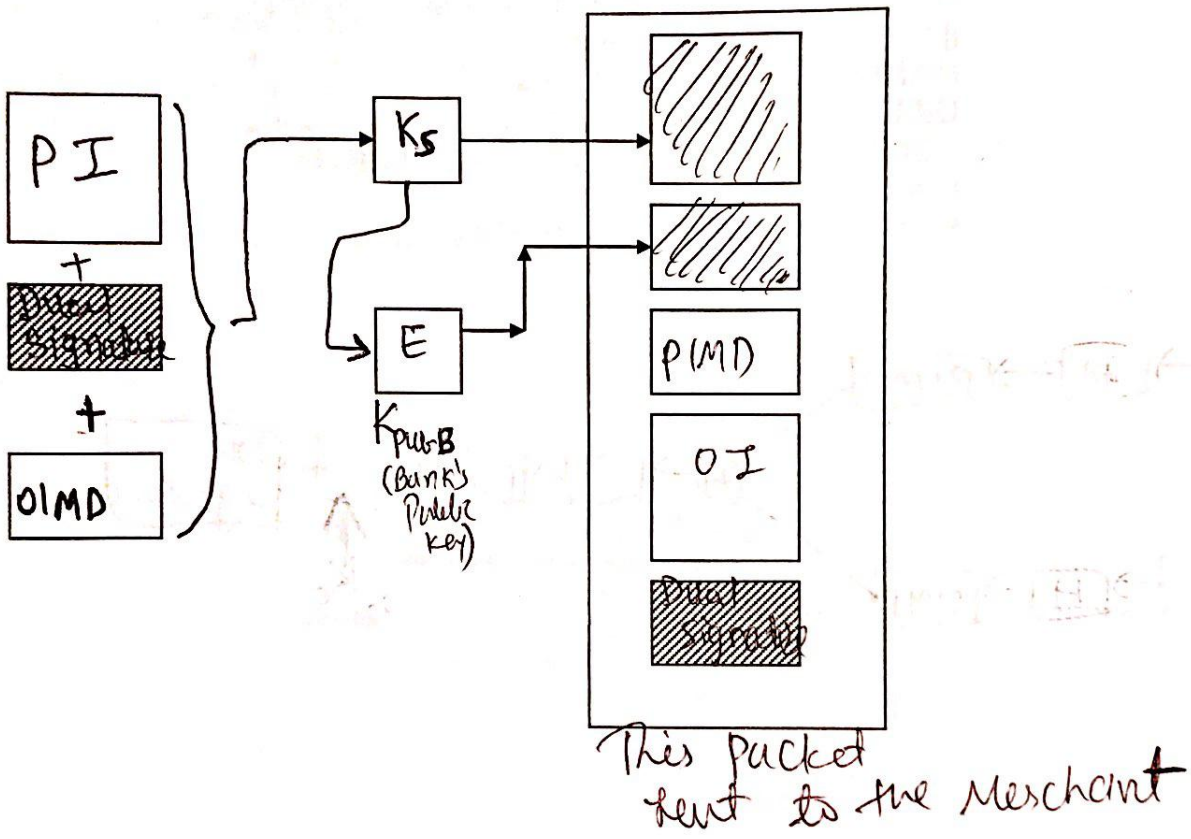
- Order Information must be verified by the merchant.
- Payment information must be verified by the issuer.

| | | |
|---|---|---|
| Let | PI = | Payment information |
| | OI = | Order information |
| | H = | Hash function (for message digest) |
| | \|\| = | Concatenation |
| | PIMD = | PI Message Digest |
| | OIMD = | OI Message Digest |
| | POMD = | Payment Order Message Digest |
| | E = | RSA Encryption |
| | Kc = | Customer's private key |



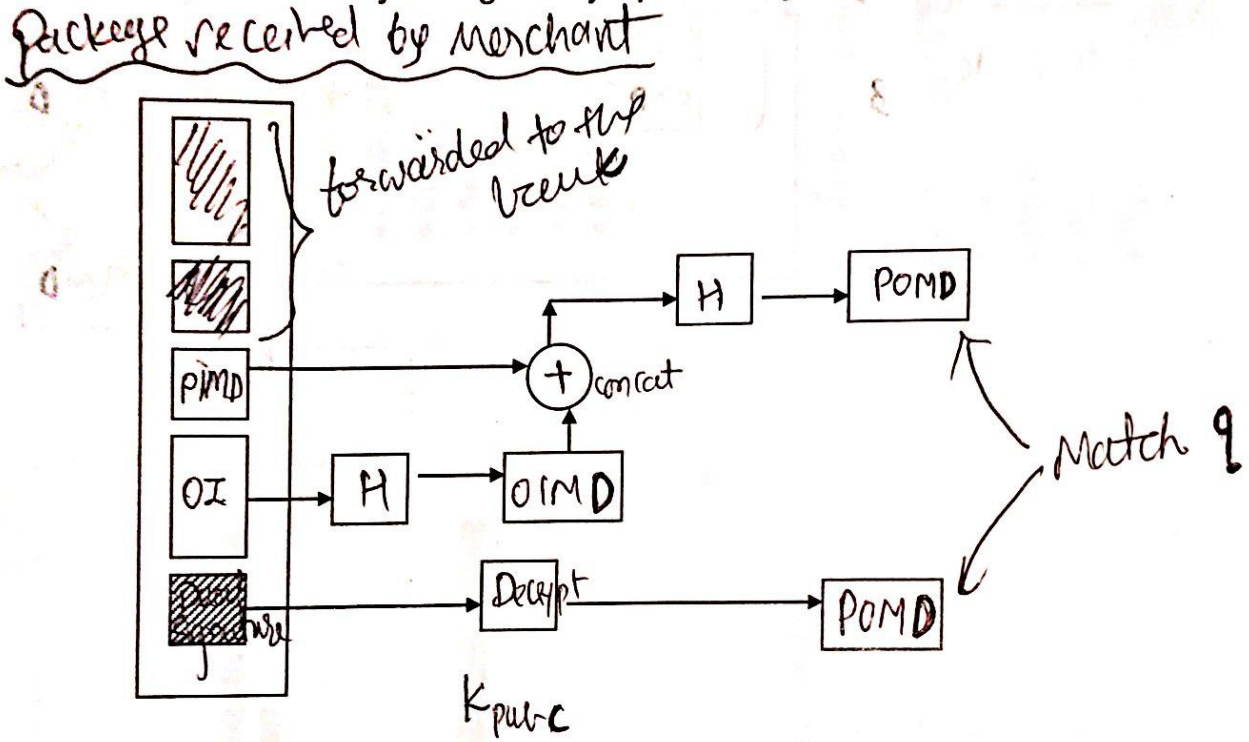
## Process- Step 1: Cardholder sends Purchase Request

| | |
|---|---|
| PI= | Payment information |
| OI= | Order information |
| PIMD= | PI message digest |
| OIMD= | OI message digest |
| E= | Encryption (RSA or DES) |
| Ks= | Temporary symmetric key |
| Kpubb= | Bank's (Payment Gateway's) public key |

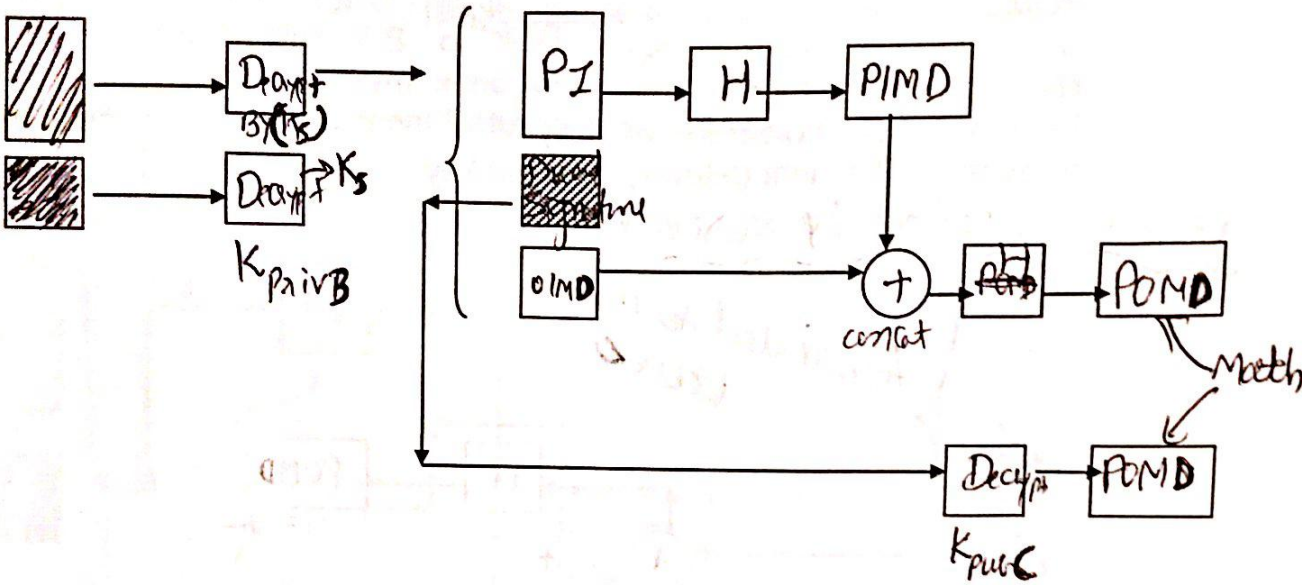


**Process – Step 2: Merchant verifies customer purchase request (order information)**

| | |
|---|---|
| OI = | Order Information |
| OIMD= | OI Message Digest |
| POMD = | Payment order message digest |
| D= | Decryption (RSA) |
| H= | Hash function |
| Kpubc= | Cardholder's public key |
| Kprivb= | Payment gateway's private key |



**Process- Step 3: Payment gateway verifies customer payment request (payment information)**



DALHOUSIE UNIVERSITY
Inspiring Minds

## Module 9: Establishing an Organization-wide Security Plan

Srini Sampalli
Professor
Faculty of Computer Science
srini@cs.dal.ca

## *Security Plan Overview*

***"Live" document that addresses how an organization will address its security.***

***It consists of:***

- ***Organization's security policy***
- ***Current state of security***
- ***Needs***
- ***Recommendations***
- ***Timeline for implementation***
- ***Evaluation plan***

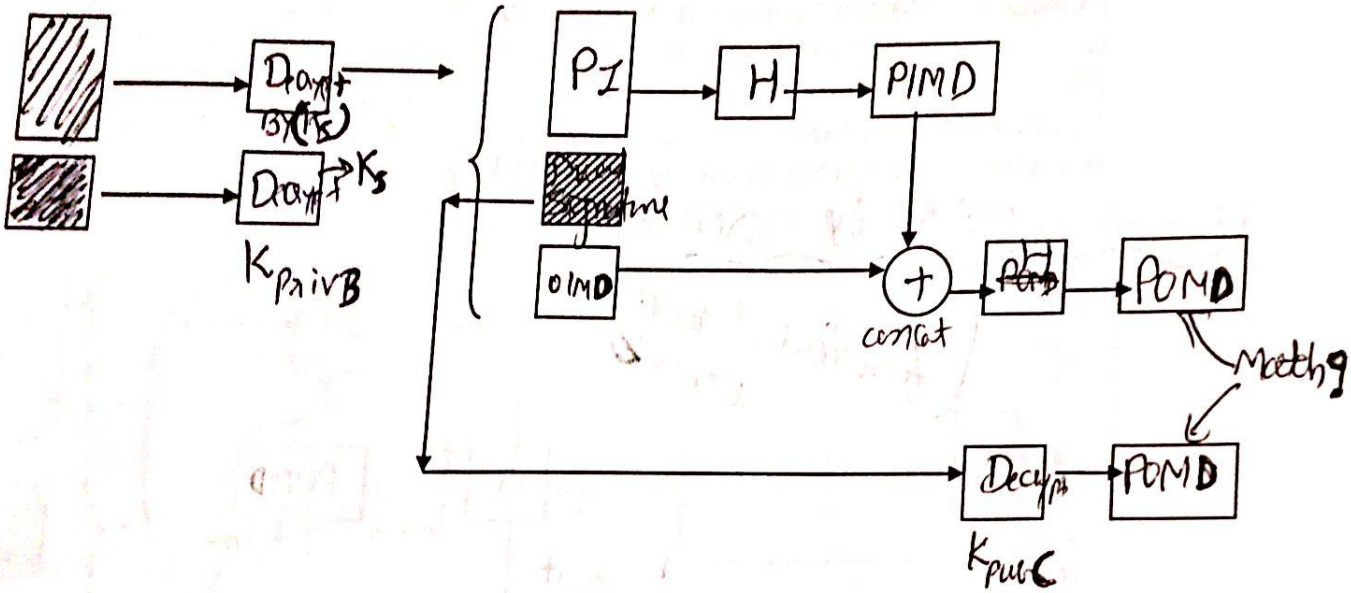
## *Questions to be addressed → The five phases of a security plan*

- ***What*** needs to be protected? → Inspection
- How to ***protect***? → Protection
- How to ***detect*** intrusion? → Detection
- How to ***react*** to a network attack? → Reaction
- How to ***recover*** from the network attack? → Reflection

## *The five phases of a security plan*

- Phase 1: Inspection
- Phase 2: Protection
- Phase 3: Detection
- Phase 4: Reaction
- Phase 5: Reflection

**Process- Step 3: Payment gateway verifies customer payment request (payment information)**



DALHOUSIE UNIVERSITY
Inspiring Minds

# Module 9: Establishing an Organization-wide Security Plan

Srini Sampalli
Professor
Faculty of Computer Science
srini@cs.dal.ca

## *Security Plan Overview*

***"Live" document that addresses how an organization will address its security.***

***It consists of:***

- ***Organization's security policy***
- ***Current state of security***
- ***Needs***
- ***Recommendations***
- ***Timeline for implementation***
- ***Evaluation plan***

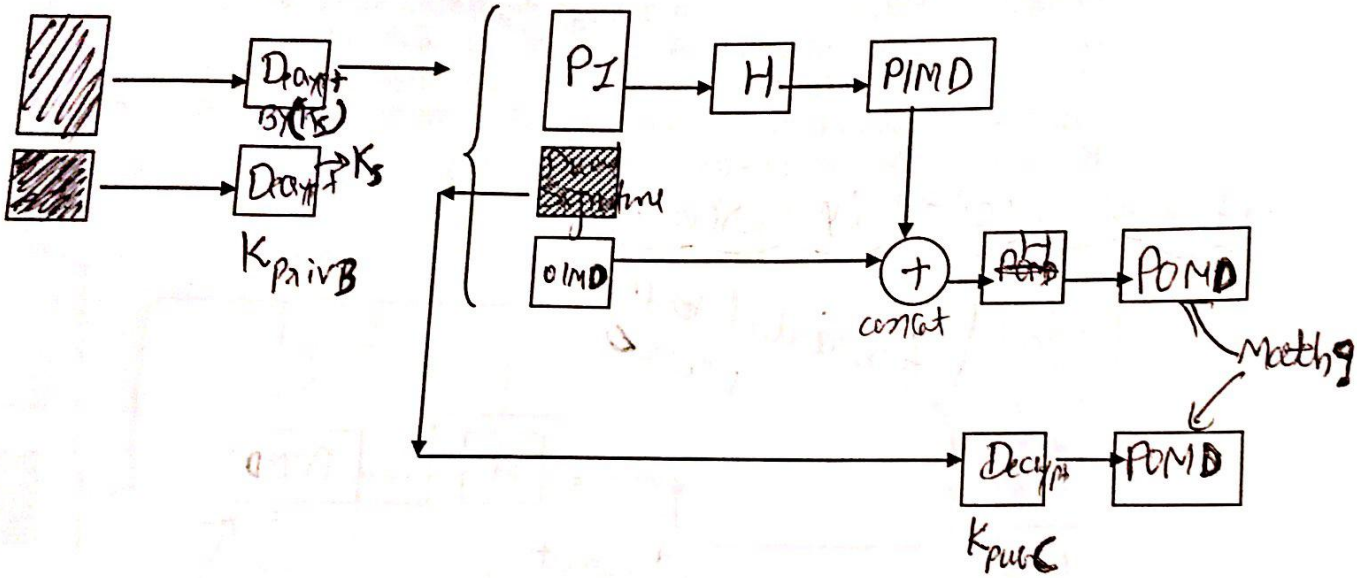
## *Questions to be addressed → The five phases of a security plan*

- ***What*** needs to be protected? → Inspection
- How to ***protect***? → Protection
- How to ***detect*** intrusion? → Detection
- How to ***react*** to a network attack? → Reaction
- How to ***recover*** from the network attack? → Reflection

## *The five phases of a security plan*

- Phase 1: Inspection
- Phase 2: Protection
- Phase 3: Detection
- Phase 4: Reaction
- Phase 5: Reflection

**Process- Step 3: Payment gateway verifies customer payment request (payment information)**



DALHOUSIE UNIVERSITY
Inspiring Minds

# Module 9: Establishing an Organization-wide Security Plan


Srini Sampalli
Professor
Faculty of Computer Science
srini@cs.dal.ca


## Security Plan Overview

*"Live" document that addresses how an organization will address its security.*

*It consists of:*

- *Organization's security policy*
- *Current state of security*
- *Needs*
- *Recommendations*
- *Timeline for implementation*
- *Evaluation plan*

9

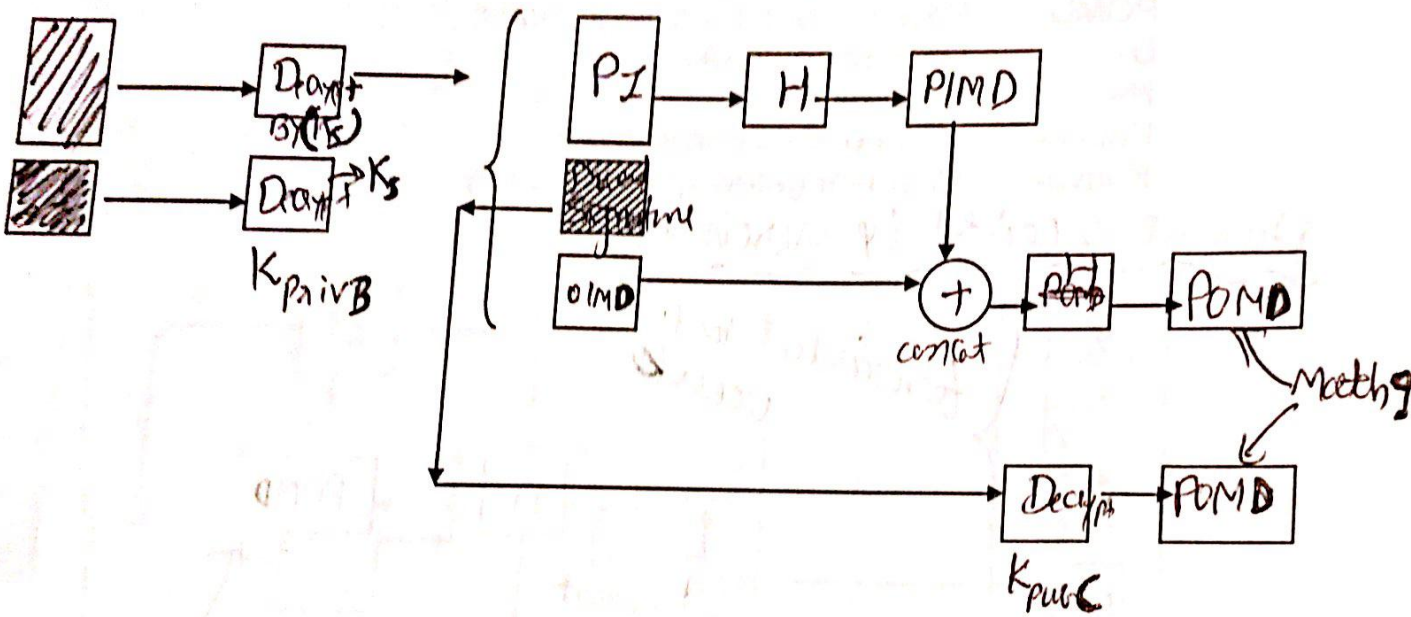
## Questions to be addressed → The five phases of a security plan

- ***What*** needs to be protected? → Inspection
- How to ***protect***? → Protection
- How to ***detect*** intrusion? → Detection
- How to ***react*** to a network attack? → Reaction
- How to ***recover*** from the network attack? → Reflection

## The five phases of a security plan

- Phase 1: Inspection
- Phase 2: Protection
- Phase 3: Detection
- Phase 4: Reaction
- Phase 5: Reflection

**Process- Step 3: Payment gateway verifies customer payment request (payment information)**



## Inspection (a.k.a. Risk Analysis)

- *Make a formal inventory of all resources (information, software, equipment, algorithms)*
- *Assign ownership to each resource (creator, maintainer, user)*
- *Determine value of each resource*
- *For each resource, list the threats that could cause damage.*
- *Calculate the risk impact, risk probability, risk exposure and risk leverage for each resource.*

① Risk Impact (R.I.) → cost to replace resource.

② Risk Probability (R.P.) → Probability of attack on resource.

③ Risk Exposure :- (RE) → RI * RP

④ Risk Leverage (RL) :- $$\frac{(RE \text{ before security}) - (RE \text{ after security})}{\text{cost of security.}}$$

Leverage tells you there, is it worth about security?

Example

cost of resource = $10000
RP1 = Chance of attack = 50%.
cost of Security S1 = $500
Chance of attack after security RP1' = 20%.

$$RL1 = \frac{(10{,}000 * 0.5) - (10{,}000 * 0.2)}{500}$$

$$= \frac{5000 - 2000}{500}$$

$$= 6$$

C1 = $100000
RP2 = 30%.
S2 = $10,000
RP2' = 10%.

$$RL2 = \frac{(100000 * 0.3) - (10{,}000 * 0.1)}{10{,}000}$$

$$= \frac{30000 - 10000}{10{,}000}$$

$$= 2$$

We'll prefer (10) C1 bcz RL is more

## 2. Protection

- Deploy tools for achieving the seven security goals for each resource or set of resources, starting with the ones with the ***highest risk leverage***.
  - Confidentiality
  - Integrity
  - Authentication
  - Non-repudiation
  - Certification
  - Access Control
  - Availability

## 3. Detection – some tools

- ***Signature Analysis***
  - Collection of event log data and comparison with predefined attack signatures.
- ***Anomaly Detection***
  - Look for unusual activities or statistically anomalous behaviour.
- ***Dynamic analysis = Signature analysis + Anomaly detection***
  - Determine if an attack is underway; tools utilize audit trails and network traffic logs.
- ***Honey Pots***
  - Subnetworks configured with vulnerabilities but have resources of no value; can be used to study how systems are attacked.

## 4. Reaction

- Prepare strategies for incident containment.
- Prepare rapid response team (ensure availability for notification 24X7; assign authority to respond).
- Develop network disconnect plan.
- Develop rapid recovery procedures.
- Assess the damage.
- Restore information from a trusted backup copy.
- Monitor the system for indications of continued attack.

## 5. Reflection

- Assemble the information from all involved.
- Conduct post-incident briefings to gather information that was not recorded.
- Produce a technical summary that can be evaluated for applicability to other systems.
- Write an executive summary for upper management to understand the incident's issues.
- Re-evaluate the organization's security plan and make changes.