PROTECTING YOUR WEB PRESENCE BY SSL / TLS

Vins Fong
Certizen Limited
17 April 2015

CERTIZEN
The operator of Hongkong Post e-Cert services
香港郵政電子核證服務之營運商

Topics to share

- Network Security Threats
- Protection by SSL/TLS
- HTTPS and Lock Icon
- SSL Certificate
- Certification Authority
- Good Practice
- More Protection

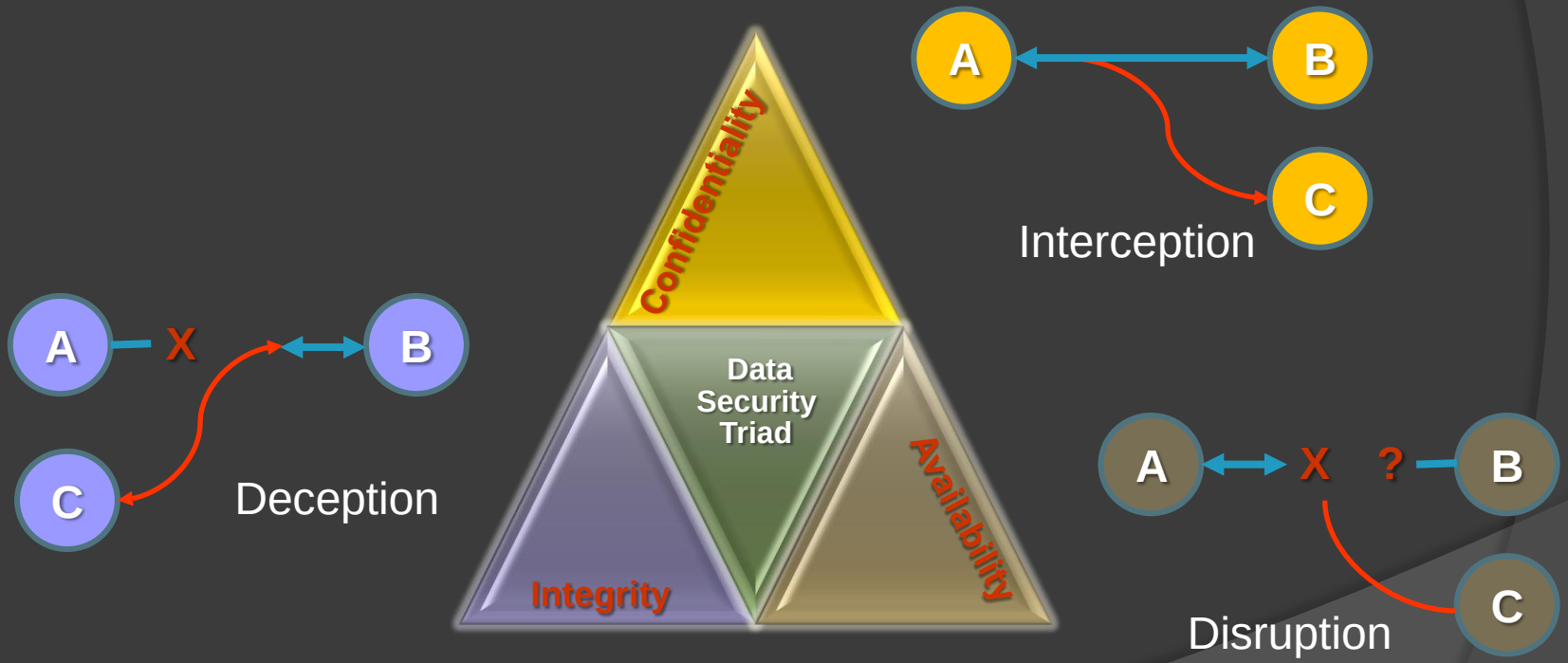
Network Security Threats

Not new issues, but becoming more risky in Internet world…

Data Security Triad

Network Security Threats

B intends to communicate with A…



Network Security Threats

How to protect …

- Availability
  - Intrusion detection/prevention system (IDS/IPS)
  - Hardware/network resilience
- Confidentiality
  - Access control system
  - Network/contents encryption

Network Security Threats

How to protect …

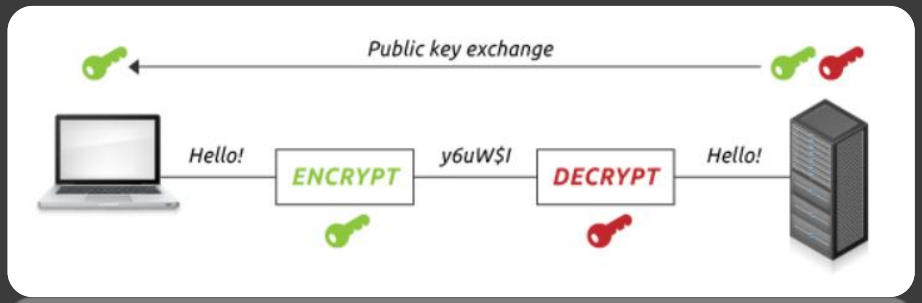
- Integrity
  - Source authentication
  - Network/contents encryption
- Non-repudiation
  - Digital signing
  - Not part of data security triad, but essential to secure electronic transactions

Protection by SSL / TLS

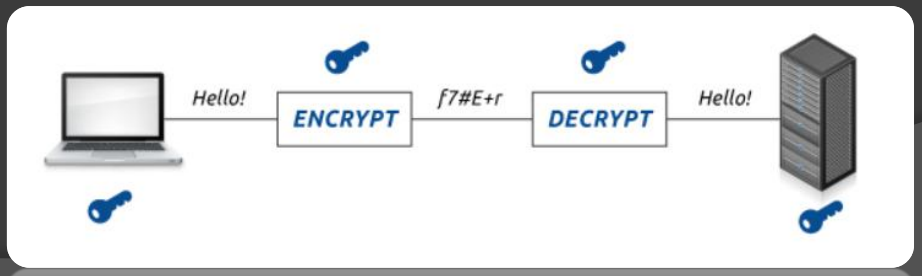
- Secure Sockets Layer (SSL) - security protocol to establish encrypted link between a server (e.g. website) and a client (e.g. browser)
- Transport Layer Security (TLS) - successor protocol of SSL, TLS v1.0 is about the same as SSL v3.1
- Cryptography is the core underlying technology

Protection by SSL / TLS

- Asymmetric encryption – more secure, demand more computing resources

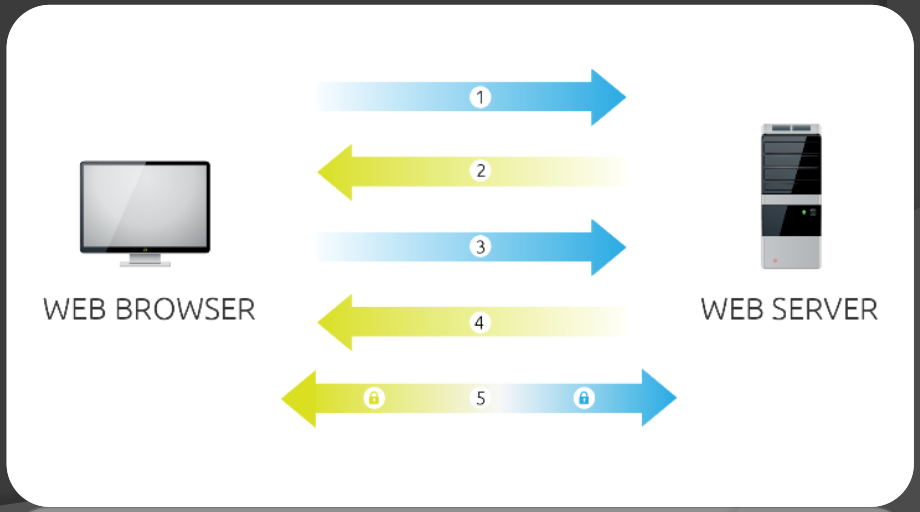


- Symmetric encryption – more efficient, less secure and less effective key handling



Protection by SSL / TLS

- SSL uses both in setting up channel-level security:
  - Uses server's asymmetric key pair for authentication and to encrypt random session key for exchange
  - Use decrypted symmetric session key to encrypt a connection session

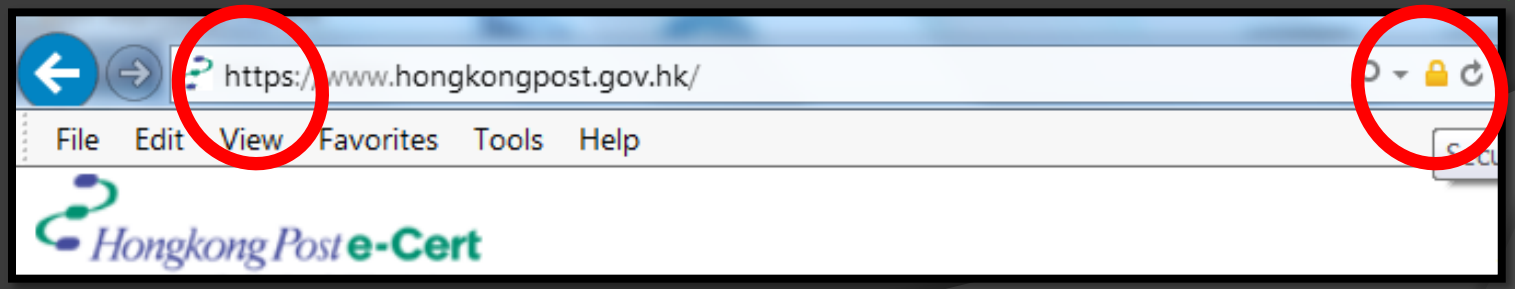


HTTPS and Lock Icon

- HTTPS – layering of standard HTTP data exchange over secure SSL/TLS connection
- Provides authentication of the visited website
- Protects confidentiality and integrity of exchanged data

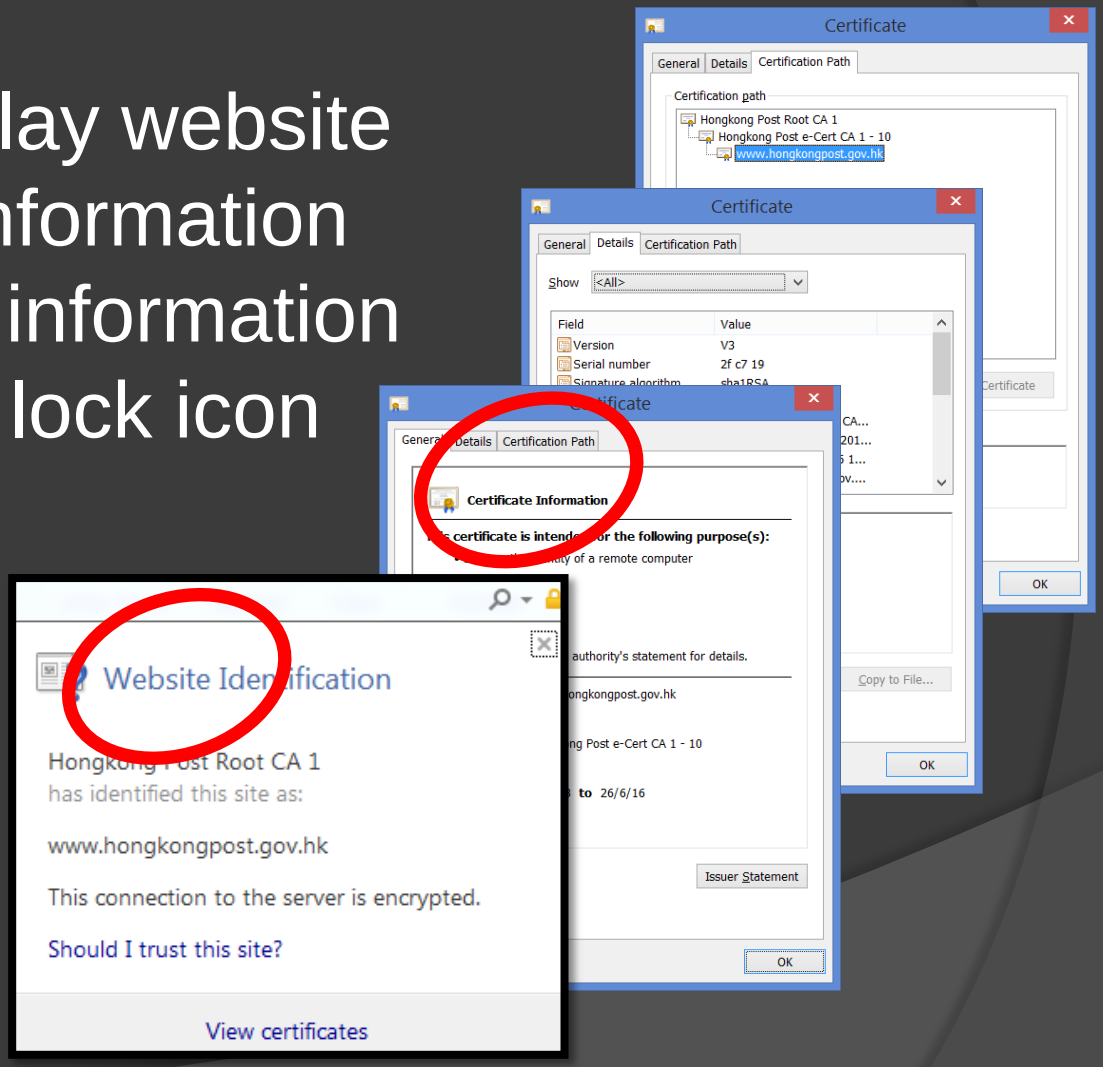
HTTPS and Lock Icon

- Lock Icon – displayed next to URL if website authentication passes:
  - SSL certificate is issued by a trusted CA
  - SSL certificate is valid
  - SSL certificate information matches domain in URL



HTTPS and Lock Icon

- User may display website identification information and certificate information by clicking the lock icon



SSL Certificate

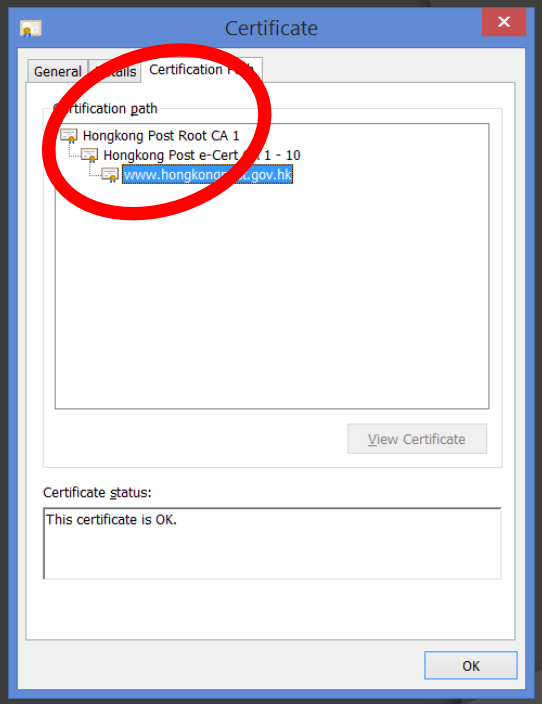
- SSL Certificate – contains key pairs, owner identity information, and digital signature of Certification Authority (CA)
- Other important attributes:
  - Format (e.g. X.509 v3)
  - Signature algorithm (e.g. SHA256 RSA)
  - Public key size 2048-bit RSA
  - Serial number, CA identity, certificate usage…

Certification Authority

- Certification Authority (CA):
  - CA digitally signs and publishes the public key bound to a given user
  - Trustworthiness of CA is most crucial
- Web of Trust:
  - CA verifies the identity of the website owner before issuing SSL certificate
  - Browser trusts the CA, trust the issuance process, thus trust the website identity

Certification Authority

- Root Certificate:
  - Self-signed certificate to identify the root CA
  - Stored at the CA in offline mode
  - The source of all trusts in PKI
- Chain of Trust
  - Certificate validity is determined by the validity of the signing certificate, bottom up to the root certificate

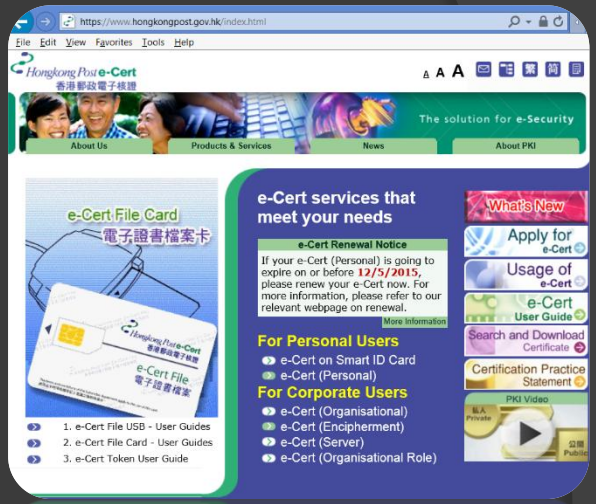


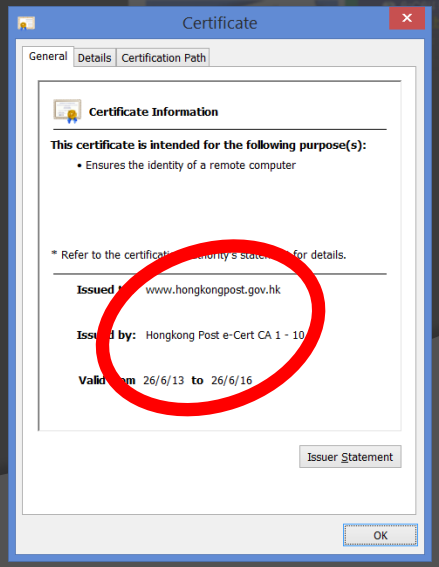
Certification Authority

- Recognized CA:
  - By virtue of Electronic Transaction Ordinance (ETO) or under Recognition Scheme
  - Comply with international standards and included in browsers' trusted root CA store
  - Possesses legal standings to prove the identify of parties involved in an electronic transaction; essential for law enforcement

Good Practice

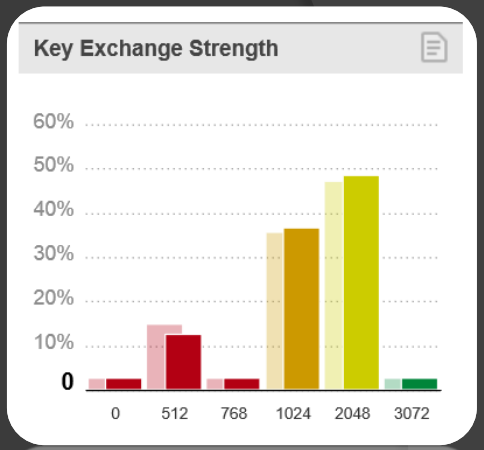
- Use certificates issued by recognized CA
- Servers: publish SSL certificate and intermediate certificates on website
- Users: check validity of website certificate and do not install untrusted certificate





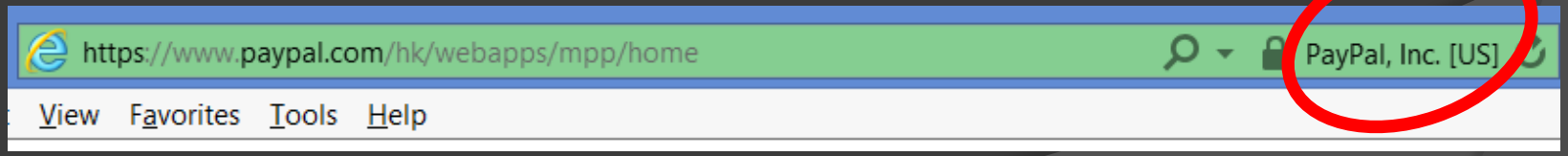
Good Practice

- Use 2048-bit encryption key:
  - Currently the minimum standards
  - RSA projected it sufficient till 2030
- Use SHA-2 signature algorithm:
  - Transition to SHA-2 is the trend
  - Microsoft and Google are going to depreciate the support of SHA-1



More Protection

- Extended Validation (EV) SSL Certificate
- Compared to SSL Certificate:
  - More extensive verification of owner identity
  - Same cryptographic strength
- Web browser could detect EV SSL certificate and show URL in green bar and location of owner



Questions are welcome
Thank you

CERTIZEN
The operator of Hongkong Post e-Cert services
香港郵政電子核證服務之營運商