ECE 671 – Lectures 20 and 21

Network security
Cryptographic Principles

Security in networks

- Where do we need … ?
  - Confidentiality
  - Integrity and non-repudiation
  - Authentication
- How to achieve … ?
  - Confidentiality
  - Integrity and non-repudiation
  - Authentication

© 2011 Tilman Wolf

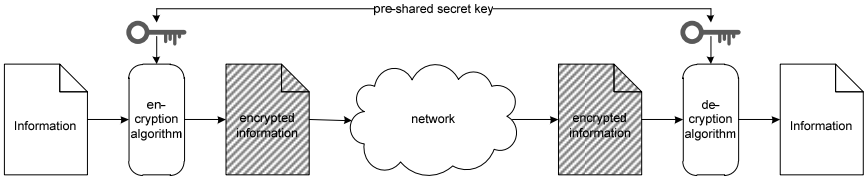
Confidentiality

- Encryption of information
- How to do encryption?

- Kerckhoffs' principle
  - System should remain secure if everything is known (except secret key)
  - Variation: security should not be based on obfuscation

Symmetric key cryptography

- Both sides use same key
  - Encryption algorithm known, key is secret
  - Key needs to be distributed a priori
- Example algorithms: DES, AES



Symmetric key cryptography

- How can we do authentication?

Symmetric key cryptography

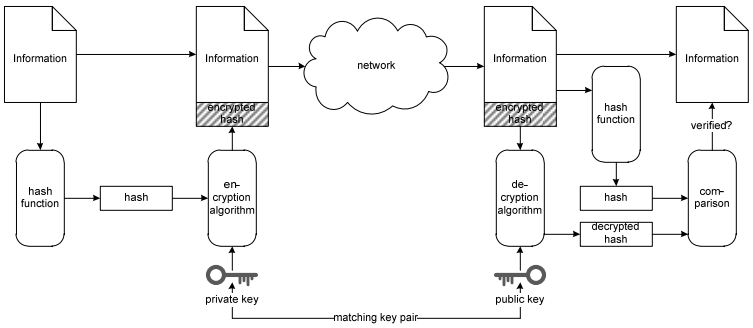
- Authentication
  - Cleartext password can be copied
  - Encrypted password is vulnerable to replay attack
- Authentication based on “challenge”
  - Random number (“nonce”) chosen by challenger
  - Other entity performs encryption using secret key
  - Replay not possible since challenge different each time

Asymmetric key cryptography

- Each entity creates two keys
  - Private key (secret), public key (widely shared)
- Encryption by one key can only be reversed by other
  - Reversal with same key computationally infeasible
  - "One-way function"
- Variety of uses can provide CIA properties
- Example algorithm: RSA

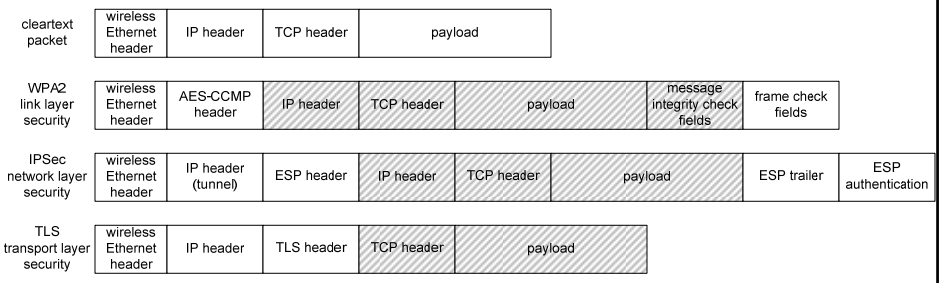
Asymmetric key cryptography

- Example: digital signature
  - Provides integrity and non-repudiation (no confidentiality)



Security in network protocols

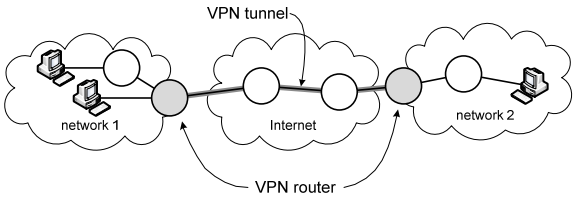
- Main focus: confidentiality
- Protocols provide security at different layers:



© 2011 Tilman Wolf

Security in network protocols

- IPSec provides security between network

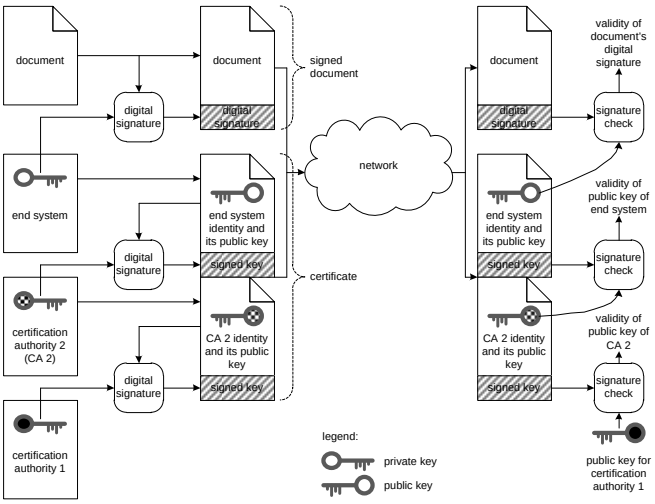


- TLS / SSL provides security between sockets
  - Security between end-systems
  - "Lock icon" in browser
  - How to establish trust with new end-system?

© 2011 Tilman Wolf

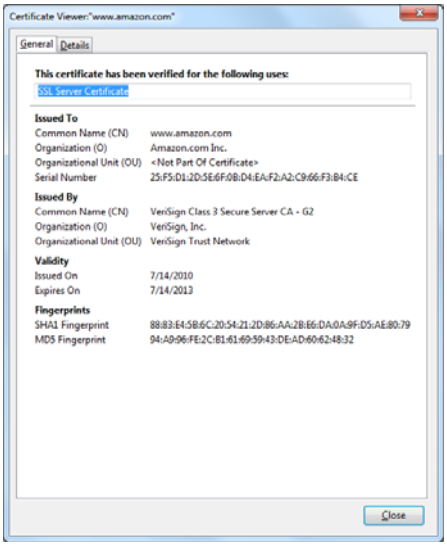
Certificates in networks

- How to trust a previously unknown entity?
- Chain of trust
  - Certification authority "signs off" on entity



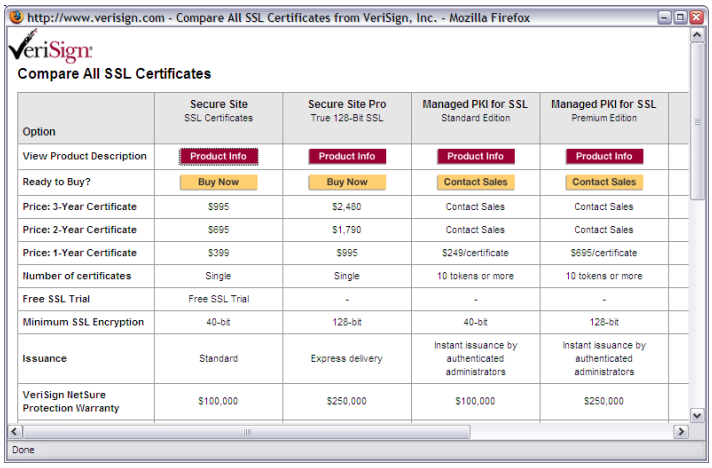
Certificate example

- Multiple certificate authorities
  - E.g., VeriSign
- Example VeriSign certificate:



SSL certificates

- Certification as a business:



Option	Secure Site SSL Certificates	Secure Site Pro True 128-Bit SSL	Managed PKI for SSL Standard Edition	Managed PKI for SSL Premium Edition
View Product Description	Product Info	Product Info	Product Info	Product Info
Ready to Buy?	Buy Now	Buy Now	Contact Sales	Contact Sales
Price: 3-Year Certificate	$995	$2,480	Contact Sales	Contact Sales
Price: 2-Year Certificate	$695	$1,790	Contact Sales	Contact Sales
Price: 1-Year Certificate	$399	$995	$249/certificate	$695/certificate
Number of certificates	Single	Single	10 tokens or more	10 tokens or more
Free SSL Trial	Free SSL Trial	-	-	-
Minimum SSL Encryption	40-bit	128-bit	40-bit	128-bit
Issuance	Standard	Express delivery	Instant issuance by authenticated administrators	Instant issuance by authenticated administrators
VeriSign NetSure Protection Warranty	$100,000	$250,000	$100,000	$250,000

Chain of trust

- Chain of trust can go multiple levels
  - Root certificates are final step
- Private keys need to protected well
- Security hardware:
  - Tamper-proof
  - On-board key generation
  - On-board cryptographic engine
  - E.g., IBM 4758 Cryptographic Coprocessor

- Many modern computers have security module