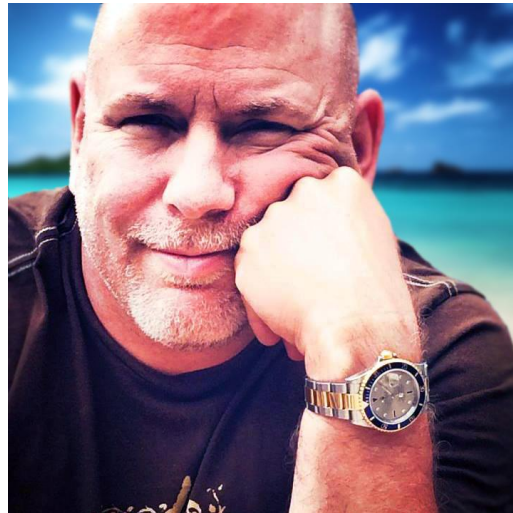


Using Appropriate Cryptographic Methods



Christopher Rees

@cdrees | <https://www.linkedin.com/in/cdrees>

Module Overview

- WEP vs. WPA/WPA2 and preshared key
- MD5
- SHA
- RIPEMD
- AES
- DES
- 3DES
- HMAC
- RSA
- Diffie-Hellman
- RC4
- One-time pads
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- TwoFish
- DHE
- ECDHE
- CHAP
- PAP
- Comparative strengths and performance of algorithms
- Use of algorithms/protocols with transport encryption
 - SSL
 - TLS
 - IPsec
 - SSH
 - HTTPS
- Cipher suites
 - Strong vs. weak ciphers
- Key stretching
 - PBKDF2
 - Bcrypt

WEP/WPA/WPA2

- Wireless access
 - WEP can be cracked **easily**
 - RC4 stream cipher
 - WPA was a **temporary** replacement for WEP
 - WPA had RC4 with TKIP
 - WPA2 **latest** standard
 - AES replaced RC4
 - CCMP replaced TKIP
 - WPA2 Enterprise
 - **RADIUS** authentication



Hashing Algorithms

- MD5
 - 128-bit
- SHA
 - SHA1 – 160-bit, SHA256 and SHA512
- RIPEMD
 - RACE Integrity Primitives Evaluation Message Digest
 - 128, 160, 256 and 320-bit versions
- HMAC
 - Hash-based Message Authentication Code
 - Uses hashing function plus secret key
 - Hashing function that verifies integrity and authentication



Symmetric Key Encryption

- DES
 - Data Encryption Standard
 - 56-bit key
- 3DES
 - 3 DES keys to encrypt data
- AES
 - Advanced Encryption Standard
 - 128-bit fixed block size
 - 10 cycles of repetition for 128-bit keys
 - 12 cycles of repetition for 192-bit keys
 - 14 cycles of repetition for 256-bit keys



Asymmetric Key Encryption

- RSA
 - Rivest, Shamir, Adleman
 - Digital Signatures
- Diffie-Hellman
 - Keying material used to generate session keys
- DHE
 - Ephemeral Diffie-Hellman
- ECDHE
 - Elliptic-Curve Diffie-Hellman



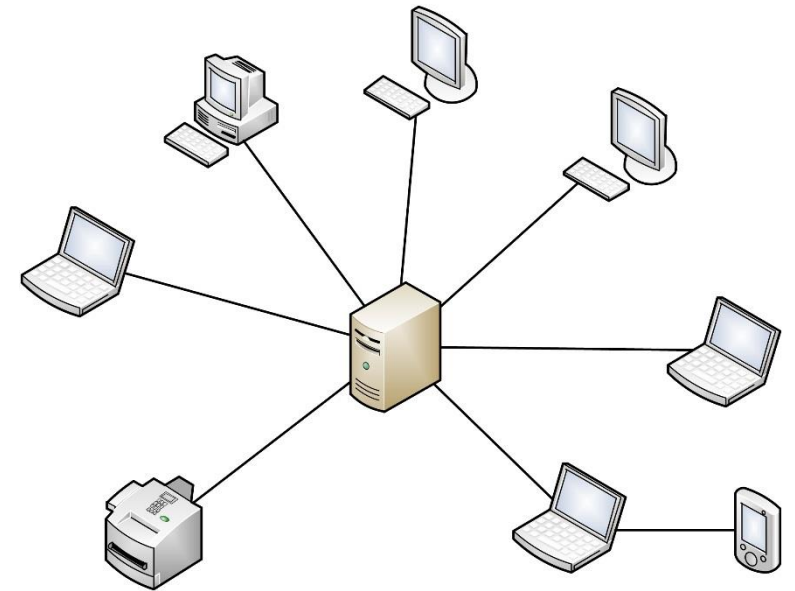
One-time Pads

- One-time pads are used for a **single communication session** and **never reused** again
 - Originated with sender and recipient having encryption key written on a pad of paper
 - Encryption key (Pad) changed each time a communication was sent



NTLM/NTLMv2

- LAN Manager
 - Originally developed by Microsoft for their early network operating systems
- NTLM
 - Used as authentication protocol in early Microsoft OS versions
- NTLMv2
 - Introduced with Windows NT4
- Kerberos
 - Replaced NTLM but NTLM still used in certain situations



Blowfish

- Symmetric key block cipher
 - Developed in 1993 by Bruce Schneier
 - 64-bit block size with variable key length from 32-bits to 448-bits
- Originally designed as a **fast, free replacement** for DES
 - Patent-free / license-free
- TwoFish and ThreeFish are the recommended replacements for Blowfish
 - Blowfish is **still** widely in use

PGP/GPG

- PGP (Pretty Good Privacy)
 - Developed by Phil Zimmerman in 1991
 - Concept of the “Web of Trust” (WoT)
- Combines several algorithms
 - Hashing
 - Data compression
 - Symmetric-key cryptography
 - Public-key cryptography



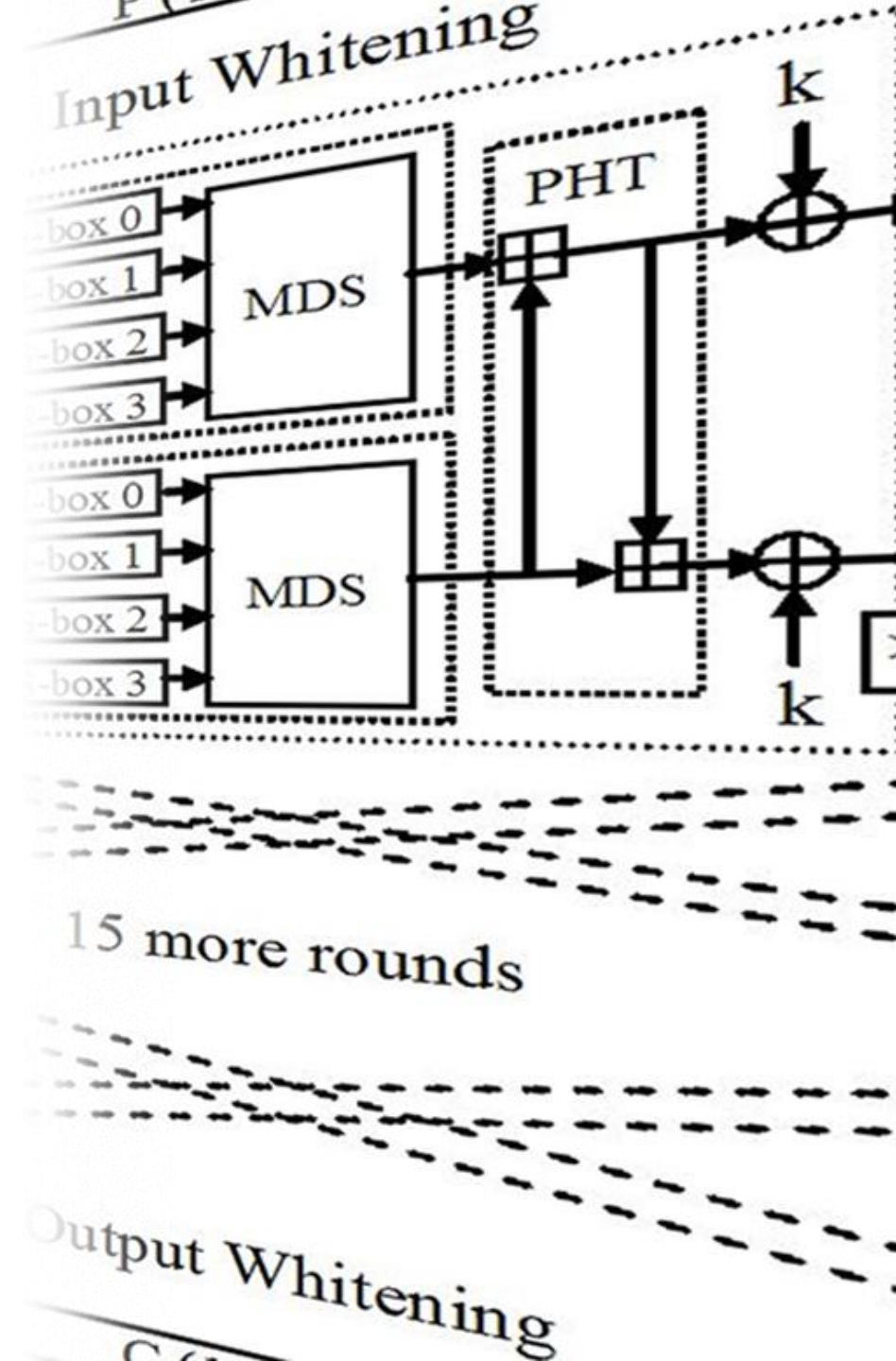
PGP/GPG

- GPG (GNU Privacy Guard)
 - Free implementation of the OpenPGP standard
 - Command line tool
- Compatible with PGP
 - Supports RSA, DES, 3DES, Blowfish, TwoFish and many others
 - Supports many graphical frontends, email and chat programs, etc



TwoFish

- Successor to Blowfish
- **Symmetric** key block cipher
 - 128-bit block size and key sizes up to 256-bit



PAP and CHAP

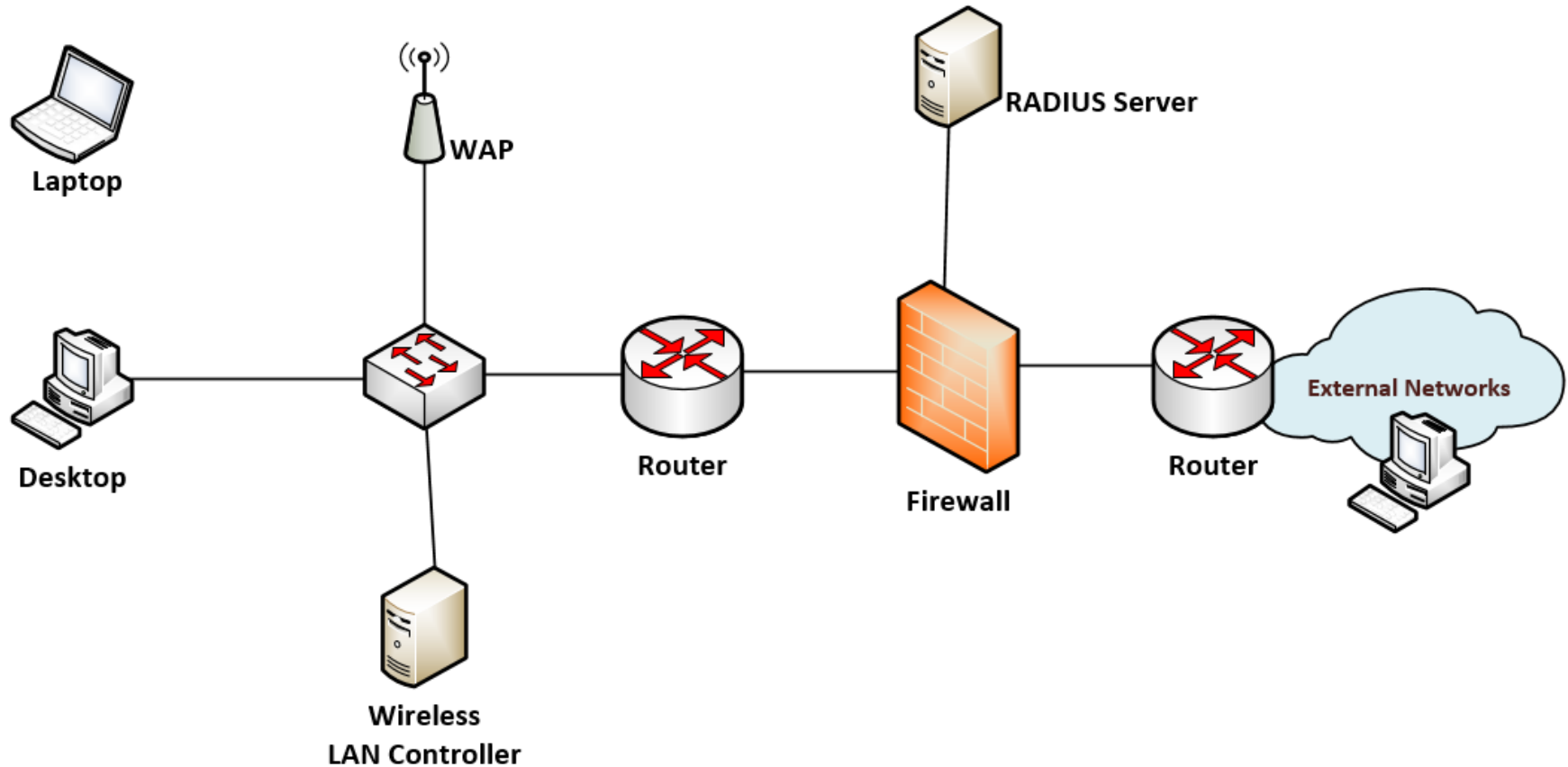
- Authentication mechanisms used in conjunction with the PPP protocol
 - Point-to-point protocol
- PAP (Password Authentication Protocol)
 - Sends passwords in **clear text** – no longer used
- CHAP (Challenge Handshake Authentication Protocol)
 - Sends **hash** of password across the network
 - Hashes are compared to authenticate

Strength and Performance of Algorithms

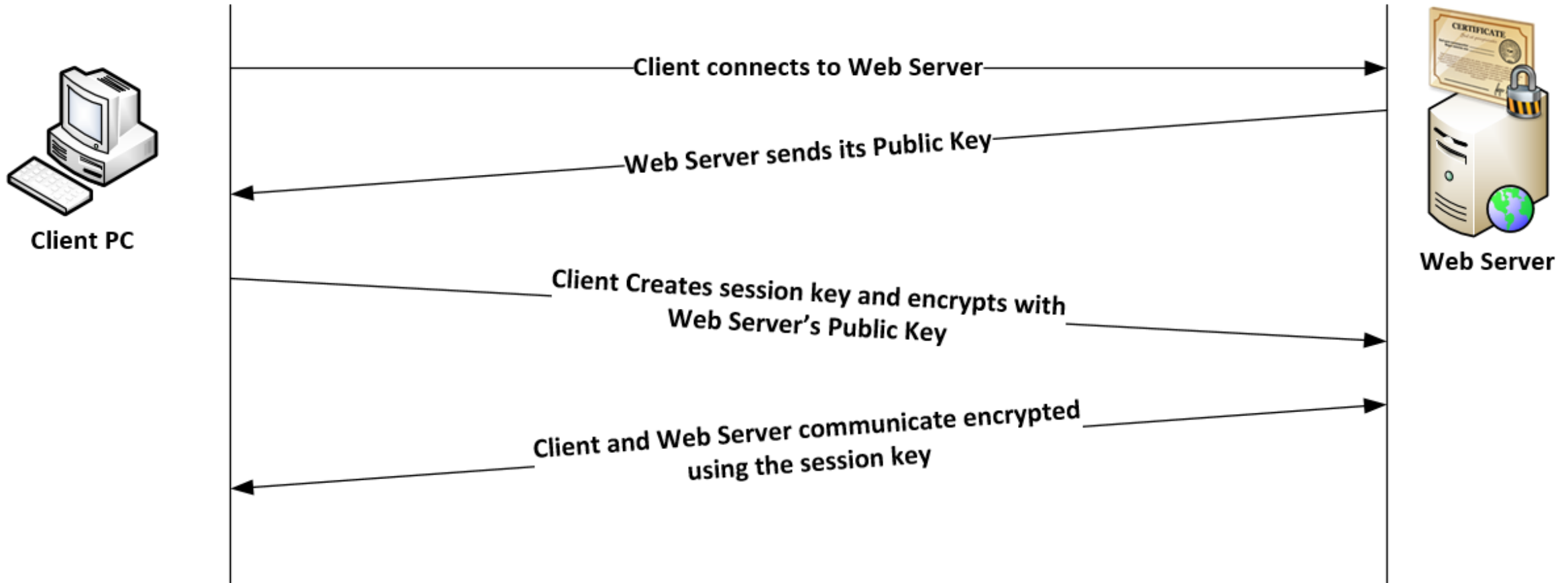
- Symmetric is **faster** than asymmetric
 - Same key for encryption and decryption
 - Bigger key sizes are more secure
 - Use more computational resources
 - Can be combined with asymmetric keys
- Asymmetric
 - Public key / Private key (mathematically linked key pair)
 - Bigger key sizes are **more secure** but use more resources

Transport Encryption

- SSL
- TLS
- IPsec
- SSH
- HTTPS



Transport Encryption



Cipher Suites

- Strong vs. weak ciphers
 - Computational resources/capabilities continue to increase
 - Strong ciphers can become weak (or weaker) as computing power increases
- Current examples of strong ciphers
 - AES
 - 3DES
 - TwoFish
- Weak ciphers
 - WEP

Key Stretching

- PBKDF2
 - Password-Based Key Derivation Function 2
 - Part of RSA (PKCS #5 v2.0)
- **Pseudorandom** function applied to password or passphrase
 - Hash, cipher or HMAC
 - **Salt** added as well for additional randomness
 - Process repeated many times
- Creates a **derived** key
 - Can be used as a cryptographic key for subsequent sessions

Key Stretching

- Bcrypt
 - Based on Blowfish algorithm (created in 1999)
 - Key derivation function used for passwords
 - Adds additional **salt function** to guard against rainbow table attacks



Module Review

- WEP vs. WPA/WPA2 and preshared key
- MD5
- SHA
- RIPEMD
- AES
- DES
- 3DES
- HMAC
- RSA
- Diffie-Hellman
- RC4
- One-time pads
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- TwoFish
- DHE
- ECDHE
- CHAP
- PAP
- Comparative strengths and performance of algorithms
- Use of algorithms/protocols with transport encryption
 - SSL
 - TLS
 - IPsec
 - SSH
 - HTTPS
- Cipher suites
 - Strong vs. weak ciphers
- Key stretching
 - PBKDF2
 - Bcrypt