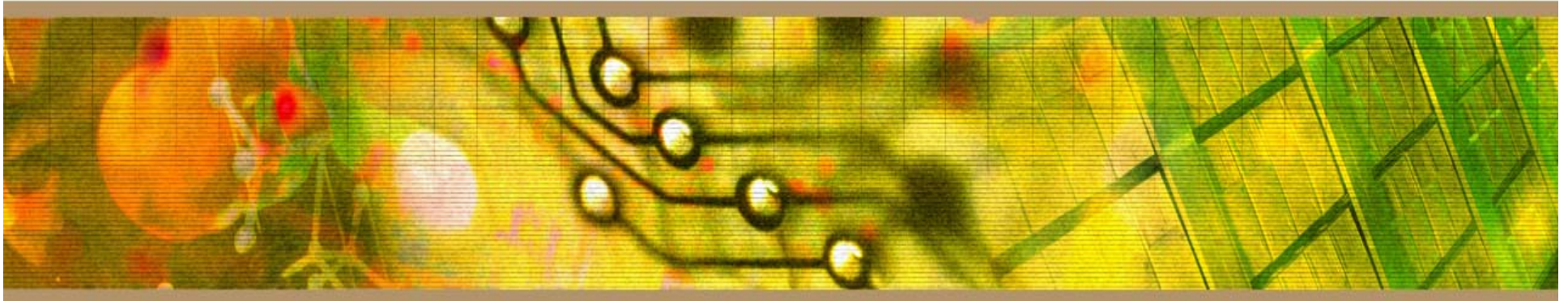




IT Networks & Security CERT Luncheon Series: Cryptography



Presented by

Addam Schroll, IT Security & Privacy Analyst



- History
- Terms & Definitions
- Symmetric and Asymmetric Algorithms
- Hashing
- PKI Concepts
- Attacks on Cryptosystems

- “Hidden writing”
- Increasingly used to protect information
- Can ensure confidentiality
 - Integrity and Authenticity too

- Dates back to at least 2000 B.C.
- Pen and Paper Cryptography
- Examples
 - Scytale
 - Atbash
 - Caesar
 - Vigenère

- Invention of cipher machines
- Examples
 - Confederate Army's Cipher Disk
 - Japanese Red and Purple Machines
 - German Enigma

- Computers!
- Examples
 - Lucifer
 - Rijndael
 - RSA
 - ElGamal

Plaintext – A message in its natural format readable by an attacker

Ciphertext – Message altered to be unreadable by anyone except the intended recipients

Key – Sequence that controls the operation and behavior of the cryptographic algorithm

Keyspace – Total number of possible values of keys in a crypto algorithm

PURDUE Speak Like a Crypto Geek (2)

UNIVERSITY

Initialization Vector – Random values used with ciphers to ensure no patterns are created during encryption

Cryptosystem – The combination of algorithm, key, and key management functions used to perform cryptographic operations

- Confidentiality
- Integrity
- Authenticity
- Nonrepudiation
- Access Control

- Stream-based Ciphers
 - One at a time, please
 - Mixes plaintext with key stream
 - Good for real-time services
- Block Ciphers
 - Amusement Park Ride
 - Substitution and transposition

- Substitution Cipher
 - Convert one letter to another
 - Cryptoquip
- Transposition Cipher
 - Change position of letter in text
 - Word Jumble
- Monoalphabetic Cipher
 - Caesar

- Polyalphabetic Cipher
 - Vigenère
- Modular Mathematics
 - Running Key Cipher
- One-time Pads
 - Randomly generated keys

- Hiding a message within another medium, such as an image
- No key is required
- Example
 - Modify color map of JPEG image

- ***Symmetric***
 - Same key for encryption and decryption
 - Key distribution problem
- ***Asymmetric***
 - Mathematically related key pairs for encryption and decryption
 - Public and private keys

▪ *Hybrid*

- Combines strengths of both methods
- Asymmetric distributes symmetric key
 - » Also known as a *session key*
- Symmetric provides bulk encryption
- Example:
 - » SSL negotiates a hybrid method

▪ *Confusion*

- Change key values each round
- Performed through substitution
- Complicates plaintext/key relationship

▪ *Diffusion*

- Change location of plaintext in ciphertext
- Done through transposition

- DES
 - Modes: ECB, CBC, CFB, OFB, CM
- 3DES
- AES
- IDEA
- Blowfish

- RC4
- RC5
- CAST
- SAFER
- Twofish

- Diffie-Hellman
- RSA
- El Gamal
- Elliptic Curve Cryptography (ECC)

- MD5
 - Computes 128-bit hash value
 - Widely used for file integrity checking
- SHA-1
 - Computes 160-bit hash value
 - NIST approved message digest algorithm

■ HAVAL

- Computes between 128 and 256 bit hash
- Between 3 and 5 rounds

■ RIPEMD-160

- Developed in Europe published in 1996
- Patent-free

- Collisions
 - Two messages with the same hash value
- Based on the “birthday paradox”
- Hash algorithms should be resistant to this attack

- Small block of data generated with a secret key and appended to a message
- HMAC (RFC 2104)
 - Uses hash instead of cipher for speed
 - Used in SSL/TLS and IPSec

- Hash of message encrypted with private key
- Digital Signature Standard (DSS)
 - DSA/RSA/ECD-SA plus SHA
- DSS provides
 - Sender authentication
 - Verification of message integrity
 - Nonrepudiation

- Key Distribution Center (KDC)
 - Uses master keys to issue session keys
 - Example: Kerberos
- ANSI X9.17
 - Used by financial institutions
 - Hierarchical set of keys
 - Higher levels used to distribute lower

- All components needed to enable secure communication
 - Policies and Procedures
 - Keys and Algorithms
 - Software and Data Formats
- Assures identity to users
- Provides key management features

- Digital Certificates
 - Contains identity and verification info
- Certificate Authorities
 - Trusted entity that issues certificates
- Registration Authorities
 - Verifies identity for certificate requests
- Certificate Revocation List (CRL)

- Process to establish a trust relationship between CAs
- Allows each CA to validate certificates issued by the other CA
- Used in large organizations or business partnerships

- The study of methods to break cryptosystems
- Often targeted at obtaining a key
- Attacks may be passive or active

- Kerckhoff's Principle
 - The only secrecy involved with a cryptosystem should be the key
- Cryptosystem Strength
 - How hard is it to determine the secret associated with the system?

- Brute force
 - Trying all key values in the keyspace
- Frequency Analysis
 - Guess values based on frequency of occurrence
- Dictionary Attack
 - Find plaintext based on common words

- **Replay Attack**
 - Repeating previous known values
- **Factoring Attacks**
 - Find keys through prime factorization
- **Ciphertext-Only**
- **Known Plaintext**
 - Format or content of plaintext available

- Chosen Plaintext
 - Attack can encrypt chosen plaintext
- Chosen Ciphertext
 - Decrypt known ciphertext to discover key
- Differential Power Analysis
 - Side Channel Attack
 - Identify algorithm and key length

- Social Engineering
 - Humans are the weakest link
- RNG Attack
 - Predict IV used by an algorithm
- Temporary Files
 - May contain plaintext

- Privacy Enhanced Email (PEM)
- Pretty Good Privacy (PGP)
 - Based on a distributed trust model
 - Each user generates a key pair
- S/MIME
 - Requires public key infrastructure
 - Supported by most e-mail clients

- Link Encryption
 - Encrypt traffic headers + data
 - Transparent to users
- End-to-End Encryption
 - Encrypts application layer data only
 - Network devices need not be aware

- SSL/TLS
 - Supports mutual authentication
 - Secures a number of popular network services

- IPSec
 - Security extensions for TCP/IP protocols
 - Supports encryption and authentication
 - Used for VPNs

Questions?