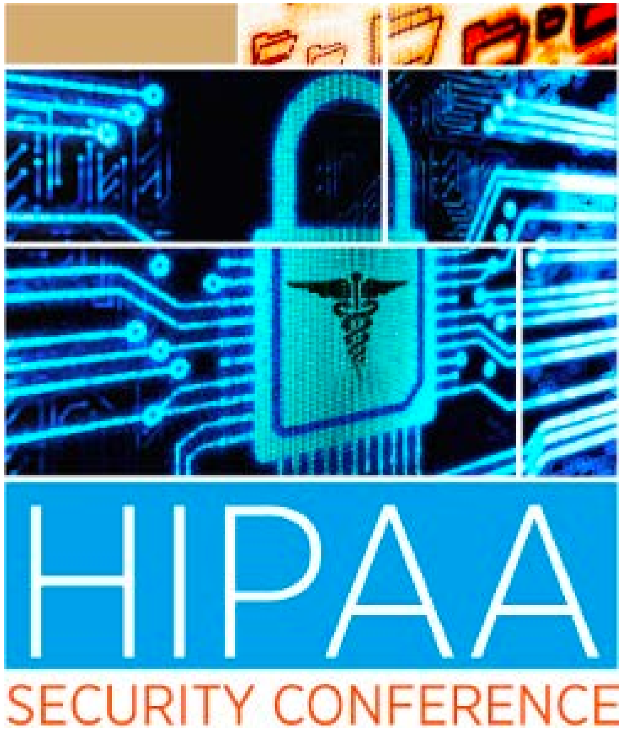
Safeguarding Data Using Encryption

Matthew Scholl &
Andrew Regenscheid
Computer Security Division, ITL, NIST



NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

What is Cryptography?

- **Cryptography**:
  "The discipline that embodies principles, means, and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity."
  NIST SP 800-21
- Covers a broad set of mathematical techniques to achieve different properties
  - *Encryption* is to provide confidentiality
  - Typically, techniques are used together

Why Use Crypto?

HIPAA Security Rule Technical Safeguards:

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

Why Use Crypto?

HIPAA Security Rule Technical Safeguards:

✓ **Access Control**

- ~~Audit Controls~~

✓ **Integrity**

✓ **Person or Entity Authentication**

✓ **Transmission Security**

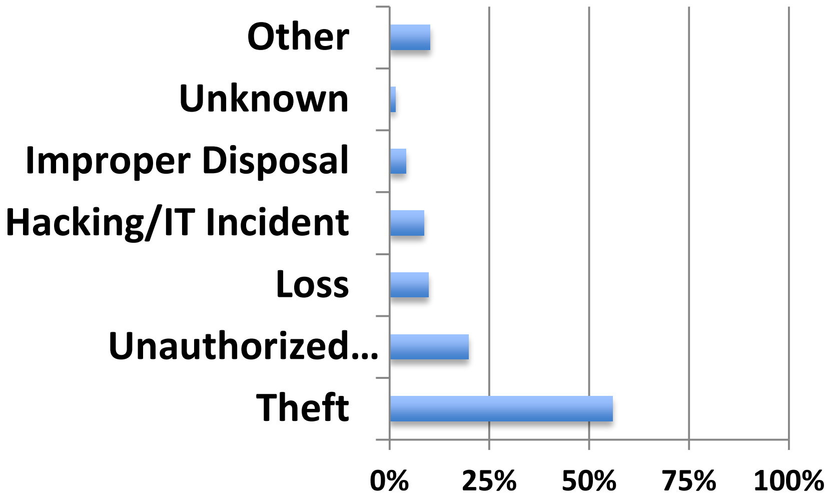
Health Information Breaches

- More than 1100 data breaches involving >500 individuals reported since HITECH Act
  - 55.9% involved theft
  - 9.75% involved loss
- Unsecured, unprotected health information

Crypto Can Help!

Data Breach Types

(1118 total events)



Occurrence Rate of Each Type

Access Control

- **Access Control Standard**

  "Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4)[Information Access Management]."

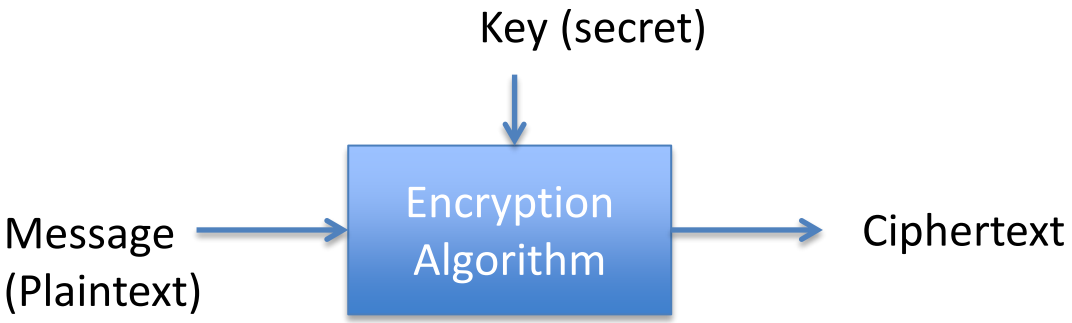
- **Implementation Specification: Encryption and Decryption**

  "Implement a mechanism to encrypt and decrypt electronic protected health information."

Encryption

- **Encryption (algorithm)**

  "Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key." CNSSI-4009



- Security based on the key secret, not the algorithm secret
- ***Examples***: AES, Triple-DES

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Integrity

- **Integrity Standard**

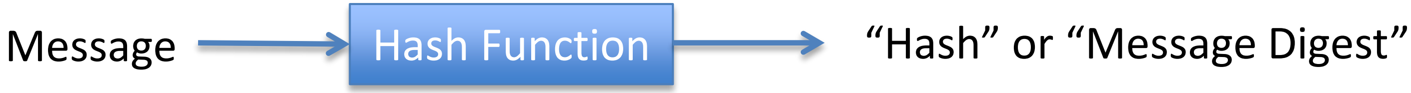
  "Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

- **Implementation Specification:** Mechanism to authenticate electronic protected health information

  "Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroy"

Hashing and MACs

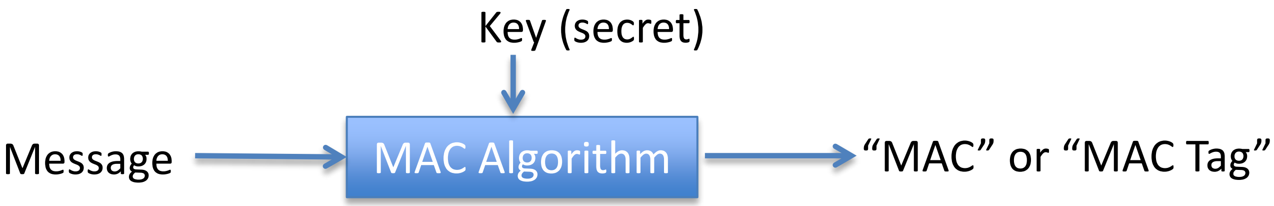
- **Hash Functions**
  - Create a short “digital fingerprint” of file or message
  - ***Highly-versatile***, but often used to verify ***integrity***



Message → Hash Function → “Hash” or “Message Digest”

  - ***Examples***: SHA-1, SHA-2

- **Message Authentication Codes (MAC)**
  - Provides ***integrity*** and ***authenticity***



Key (secret)

Message → MAC Algorithm → “MAC” or “MAC Tag”

  - ***Examples***: HMAC (w/ hash algorithm), CMAC w/ block cipher)

Person or Entity Authentication

- **Person or Entity Authentication Standard**
  “Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”

National Institute of Standards and Technology
U.S. Department of Commerce

Digital Signatures

- Digital Signatures provide ***integrity***, ***authenticity***, and ***non-repudiation*** using a digital signature algorithm and a hash function
  - Only the holder of a (private) key can generate a signature
  - Anyone can verify using a public key
- Applications
  - Device/user/entity authentication
  - Document/e-mail signing
- ***Examples***: DSA, ECDSA, RSA

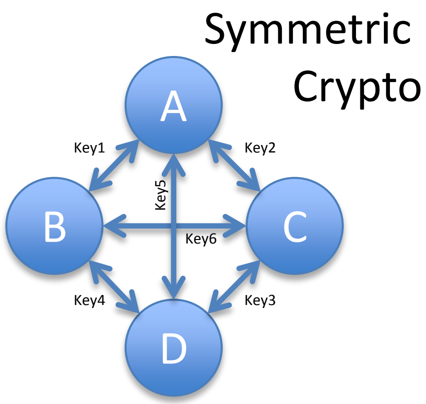
Transmission Security

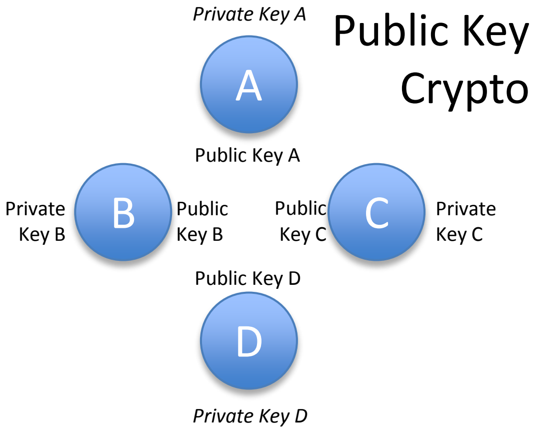
- **Transmission Security Standard**
  “Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.”
- **Implementation Specification**: Integrity controls
  Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
- **Implementation Specification**: Encryption
  “Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.”

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Key Establishment

- Basic Cryptographic Tools
  - **Encryption** provides confidentiality
  - **MAC algorithms** provide integrity
  - *But*, these need cryptographic keys
- What if you haven't distributed keys?
- Public Key Cryptography
  - Facilitates secure communication between parties who have never met
  - ***Examples***: RSA, Diffie-Hellman





NIST National Institute of Standards and Technology U.S. Department of Commerce

HIPAA and Crypto- Summary

Technical Safeguard	Supporting Cryptographic Tools
Access Control	Encryption
Integrity	Hash functions, MACs, Digital Signatures
Person or Entity Authentication	Digital Signatures
Transmission Security	Encryption, Hash functions, MACs, Digital Signatures

NIST Crypto Program

- ***Algorithm specifications:*** FIPS and Special Publications specify a number of approved cryptographic algorithms
- ***General guidance on the use of cryptography:*** Covering selection, implementation, deployment and use of cryptography.
- ***Guidelines in application-specific areas:*** Covers areas of particular need for the USG (e.g., PIV, TLS).
- ***Testing:*** Providing assurance that crypto is implemented properly (e.g., FIPS 140 and CMVP)

When Should I Use Crypto?

- Consider use of cryptography to protect any sensitive data
  - Whenever data needs to be kept confidential
  - Whenever data must be protected from modification
  - Whenever you need to verify the source of data

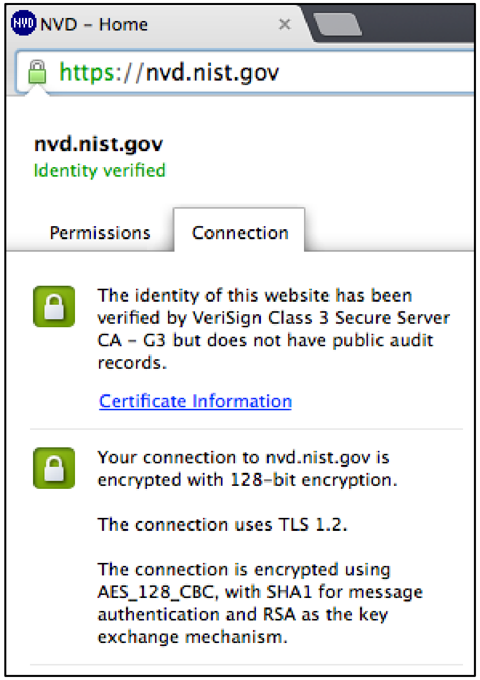
- When implemented properly, crypto should be nearly transparent to users

Data Encryption

- Provides Data-At-Rest Protection
  - Full Disk Encryption (FDE)
  - Volume Encryption
  - File/Folder Encryption
- Commonly used in laptops, mobile devices, and portable storage devices
  - Many platforms provide native FDE capabilities
- Reference:
  - NIST SP 800-111 *Guide to Storage Encryption Technologies for End User Devices*

Transport Layer Security

- Widely deployed on the Web
- Provides confidentiality and authenticity of communications
- TLS configuration can be complicated
  - *Version*: NIST recommends version1.2
  - *Cipher Suites*: NIST-approved cipher suites available
  - *Extensions:* Many, many options…
- Reference:
  - NIST SP 800-52 rev1: *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*



nvd.nist.gov
Identity verified

The identity of this website has been verified by VeriSign Class 3 Secure Server CA – G3 but does not have public audit records.

Your connection to nvd.nist.gov is encrypted with 128-bit encryption.

The connection uses TLS 1.2.

The connection is encrypted using AES_128_CBC, with SHA1 for message authentication and RSA as the key exchange mechanism.

National Institute of Standards and Technology
U.S. Department of Commerce

What is Good Crypto?

- You need confidence in:
  - Cryptographic Algorithms
  - Cryptographic Keys
  - Implementations

Selecting Crypto Algorithms

- First identity security goals
- Primary considerations for algorithms:
  - Security
  - Interoperability
  - Efficiency
- Choose from well-vetted, standardized algorithms supported by applications and users
- ***NIST Cryptographic Toolkit*** http://csrc.nist.gov/groups/ST/toolkit/

National Institute of Standards and Technology
U.S. Department of Commerce

Key Management

- Generate/establish cryptographic keys properly
- Protect the key
  - Keep it secret
  - Protect it from modification
- Transport it securely
- Know the importance of the key length

Security Strengths

- Security strengths based on the algorithm and key length
- See NIST SP 800-131A, *Transitions: Recommendation for Transition the Use of Algorithms and Key Lengths*

Strength	Encryption	Key Est./Digital Signatures	Hashing (w/ Signatures)	Hashing-Other
80 *(disallowed 2013)*		RSA-1024 ECC w/ 160 bit keys	SHA1	
112	Triple-DES (3 key)	RSA-2048 ECC w/ 224 bit keys	SHA2-224	
128	AES-128	RSA-4096 ECC w/ 256 bit keys	SHA2-256	SHA1 (160 bits)
256	AES-256	RSA-15360 ECC w/ 512 bit keys	SHA2-512	SHA2-256

FIPS 140 and CMVP

- ***FIPS 140:*** requirements in 11 areas to the design and implementation of a cryptographic module
- ***Cryptographic Module Validation Program:*** NIST/CSEC program to test modules
  - Vendors submit modules
  - Testing conducted by accredited test laboratories

CMVP
Conformance through Testing
FIPS VALIDATED 140-2

- References:
  - **CMVP**: http://csrc.nist.gov/groups/STM/cmvp/
  - **FIPS 140 Validated Modules:** http://csrc.nist.gov/groups/STM/cmvp/validation.html

Summary

- Cryptography is not a silver bullet
- But, cryptography can provide many important security properties
  - Confidentiality, Integrity, Authenticity
- To be effective, cryptographic mechanisms must be implemented properly

More Information

NIST standards and guidelines available at:

http://csrc.nist.gov

Contact Information

Andrew Regenscheid

Andrew.Regenscheid@nist.gov