A "Best Practice" Guide to Encryption for Telehealth

Liam Caffery PhD
Centre for Online Health
The University of Queensland

Overview

- Introduction
  - Current state of security in telehealth
  - Is there actually a threat?
- Background
  - Encryption terminology
  - Aim to identify metrics for risk assessment
- Review of security policy potentially affect telehealth services
- Statutory bodies
- Recommendations on "best practice"

Introduction

- Security determinant of successful telehealth [1]
- Standards-based encryption constantly changing
- Identified threats and increasing public perception
- Telehealth uses outdated security standards [2]
- Bad encryption is worse than no encryption at all
- "Best Practices" adopted by telehealth service providers

1 Broens T H F, Huis in't Veld R M H, Vollenbroek-Hutton M M R et al *Determinants of successful telemedicine implementations: a literature study* Journal of Telemedicine and Telecare 2007 13: 3030-309

2 Garg V, Brewer J *Telemedicine Security: A Systematic Review* Journal of Diabetes Science and Technology Volume 5 Issue 3, May 2011

Security threats

The data ransom first hit four Queensland medical centres a few weeks ago.

Security threats

Overview

- Introduction
  - Current state of security in telehealth
  - Is there actually a threat?
- Background
  - Encryption terminology
  - Aim to identify metrics for risk assessment
- Review of security policy potentially affect telehealth services
- Statutory bodies
- Recommendations on “best practice”

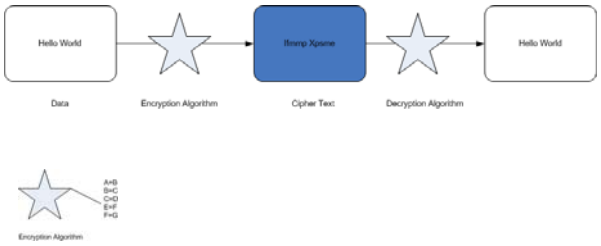
Definitions

- Encryption encoding of data into an unreadable format
- Aim of protecting from unauthorized interception and reading
- Scope
  - data at rest (files, backups)
  - data in motion (transmitted over a network)
    - Email
    - Web browsing
- Information – passwords or patient information
- Decryption decoding the data so it can be used

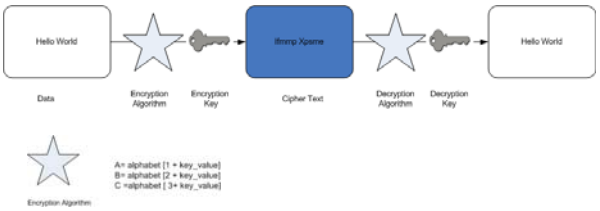
Approaches to encryption

- Encrypting network channel
  - Virtual Private Networks (VPN)
  - Wireless networks (WEP, WPA)
- Encrypting the information that is send across an unencrypted network channel
  - Email (S/MIME, OpenPGP)
  - Web services e.g. web browsing, messaging (SSL/TLS)

Encryption algorithm (ciphersuite)



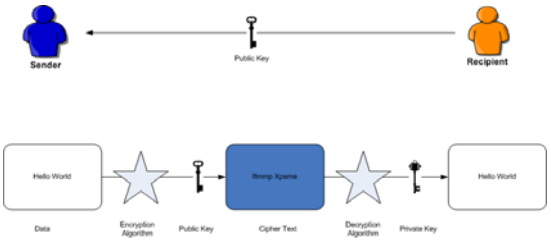
Encryption keys (certificates)



Encryption keys

- Symmetrical key cryptography
  - the same key is used to encode and decode data
- Asymmetrical key cryptography
  - encoding key is called public key
  - decoding key is called private key
  - only the private key can decode (not the public key)
  - public key and private key are mathematically related but not the same
  - public key is distributed to public
  - private key is safeguarded
  - Public Key Infrastructure (PKI)

Encryption keys



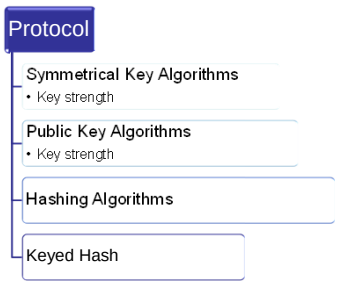
Key strength

- Key strength
  - Measured in bits
  - Longer more secure

Digest

- Message digest
  - Non repudiation
  - Hashing algorithm
  - Checksum used for “tamper checking”
  - Sender hashes unencrypted data to create message digest
  - Sends encrypted data plus message digest
  - Recipients decrypts data and re-creates message digest
  - Compares transmitted digest with re-created digest

Protocol functions



Protocol versions

Protocol	Latest version	Application
Secure Socket Layer (SSL)	3.0	Web services, web browsing, authentication services, Internet telephony, Internet video conferencing
Transport Layer Security (TLS)	1.2	As above
S/MIME	3.0	Email
OpenPGP	5.x	Email
Internet Protocol Security (IPsec)	3	Virtual Private Network (VPN)
Wi-Fi Protected Access (WPA)	2	Wi-Fi security

Different algorithms same function

Function	Algorithms	Key Strength	Protocol Applications
Symmetrical Key	Advanced Encryption Standard (AES)	256,192, 128	SSL/TLS
	Triple Data Encryption (3DES)	168, 112, 56	SSL/TLS
Public Key	Diffie-Hellman (DH)	1024	SSL/TLS
	Elliptic Diffie-Hellman (EDH)	160	SSL/TLS
	Rivest Shamir Adleman (RSA)	1024	SSL/TLS

Summary

- Encryption protocols are versioned
- Encryption protocols implemented by underlying algorithms
- Algorithms perform different functions
- One protocol can use many different algorithms for a particular function
- Algorithms have different strengths based on key size
- Evaluating a security protocol need to assess
  - Version
  - Algorithms for each function
  - Key strength of each algorithm

Overview

- Introduction
  - Current state of security in telehealth
  - Is there actually a threat?
- Background
  - Encryption terminology
  - Aim to identify metrics for risk assessment
- Review of security policy potentially affect telehealth services
- Statutory bodies
- Recommendations on “best practice”

Methods

- Review of security policy pertinent telehealth
  - **Queensland Government** *Network Transmission Security Assurance Framework*
  - **RACGP** *Computer and Information Security Standard*
  - **NEHTA** *HI Services Security and Access Framework*
  - **DICOM** *Security and System Management Profile*
  - **Standards Australia** *Information Security Management: Implementation Guide for the Health Sector*
- Encryption standards

Results

- *"All electronic communication channels will be protected with encryption techniques."*
- *"….encryption technology needs to be considered."*

Results

Cryptographic Algorithms Set 1 (CAS1) [Vulnerability Exposure = Medium]		
	Recommended algorithms	**Minimum key strength**
Public-key	RSA, D-H, ECC	160+ ECC 160+ exponent, 1024+ Modulus
Symmetric-key	3DES	80+
	AES	128 bit key or higher
Hash	SHA-1 or SHA-2, MD5	80+ (equivocal)
Keyed-hash	HMAC-SHA-1, HMAC-SHA-2	80+ (equivocal)

Results

- *Two cypher suites (algorithms) options shall be offered during TLS negotiation by applications that comply with this profile*:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA

Risk

"It is possible that relatively weak cryptographic algorithms could be selected without the user's knowledge. In combination with an assumed level of security confidence, this can represent a significant level of security risk."

Risk

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

Breaking 104 Bit WEP in Less Than 60 Seconds

Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin*

TU Darmstadt, FB Informatik
Hochschulstrasse 10, 64289 Darmstadt, Germany
{e_tews,weinmann,pyshkin}@cdc.informatik.tu-darmstadt.de

Abstract. We demonstrate an active attack on the WEP protocol that is able to recover a 104-bit WEP key using less than 40,000 frames with a success probability of 50%. In order to succeed in 95% of all cases, 85,000 packets are needed. The IV of these packets can be randomly chosen. This is an improvement in the number of required frames by more than an order of magnitude over the best known key-recovery attacks for WEP. On a IEEE 802.11g network, the number of frames required can be obtained by re-injection in less than a minute. The required computational effort is approximately 2^{20} RC4 key setups, which on current desktop and laptop CPUs is negligible.

Risk

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

On Recent Results for MD2, MD4 and MD5

Abstract. Recent cryptanalytic results on the properties of three popular hash functions have raised questions about their security. This note summarizes these results, gives our assessment of their implications and offers our recommendations for product planners and developers who may be using these algorithms.

Overview

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

- Introduction
  - Current state of security in telehealth
  - Is there actually a threat?
- Background
  - Encryption terminology
  - Aim to identify metrics for risk assessment
- Review of security policy potentially affect telehealth services
- Statutory bodies
- Recommendations on “best practice”

Statutory bodies

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

How does a telehealth provider know what protocol, version, algorithms is best practice?

- The Australian Governments Defence Signals Directorate
- Information Security Manual 2012
- DSD Approved Cryptographic Protocols
- DSD Approved Cryptographic Algorithms

www.dsd.gov.au/publications/Information_Security_manual_2012_controls.pdf

Statutory bodies

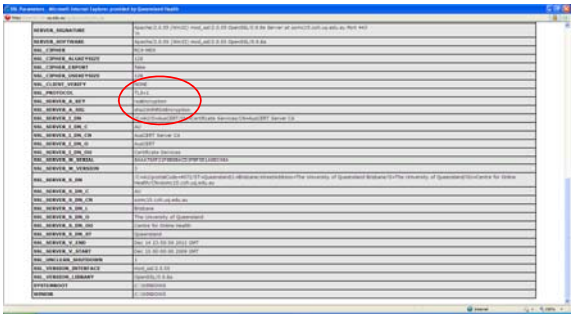
- US National Institute of Standards and Technology (NIST)
- FIPS 140-2 Security Requirement for Cryptographic Modules

Category	Approved Algorithms	Non-approved Algorithms	Application
Hashing			
	Secure Hashing Algorithm (SHA) 2 including SHA-224, SHA-256, SHA-384, SHAE-512	MD5,SHA-1	SSL/TLS, VPN
Symmetrical Key			
	Advanced Encryption Standard (AES) using a key strength 128, 192, 256	AES with a key strength less than 128	SSL/TLS, VPN
	Triple Data Encryption (3DES)		SSL/TLS, VPN
Asymmetrical Key/Public Key			
	Diffie-Hellman (DH) 1024-bits, Elliptic Diffie-Hellman (EDH) 160-bits, Rivest Shamir Adleman (RSA) 1024-bits	Key strengths less than listed.	
Key Exchange	Internet Key Exchange (IKE) Version 1 and 2, Internet Security Association Key Management Protocol (ISAKM)		VPN

Overview

- Introduction
  - Current state of security in telehealth
  - Is there actually a threat?
- Background
  - Encryption terminology
  - Aim to identify metrics for risk assessment
- Review of security policy potentially affect telehealth services
- Statutory bodies
- Recommendations on “best practice” and conclusion

Recommendations



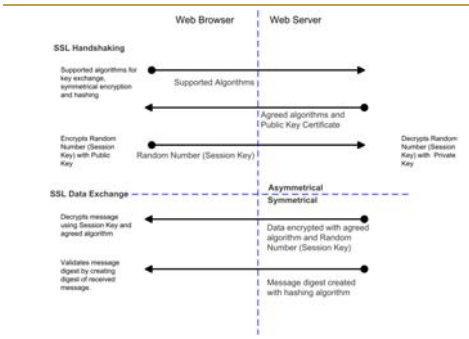
Conclusion

- Telehealth service providers aware of constantly changing nature of encryption technology
- Metrics to assess encryption include:
  - protocol version
  - algorithms for each function
  - key strength
- Functional requirement of systems encryption metrics are transparent and auditable
- Risk assessment leverage work by DFD or NIST

Contact

Liam Caffery
l.caffery@uq.edu.au
www.uq.edu.au/coh

Secure socket layer



Security threats

Hackers declare 'cyber war' on Israel after IDF threatens to cut off internet in Gaza

- **Anonymous claims to have defaced more than 650 Israeli websites**
- **Israelis deny any damage, but admit suffering 60million hack attempts**
- **Now officer says war is fought on 'three fronts' - including cyber attacks**

By DAMIEN GAYLE

PUBLISHED: 10:19 GMT, 20 November 2012 | **UPDATED:** 15:55 GMT, 20 November 2012

Comments (119) | Share | Tweet 58 | Like 463

Hackers' collective Anonymous claims it has declared 'cyber war' against Israel in retaliation for threats to block Palestinians' internet access.

As the Israel Defence Forces began airstrikes against targets in the territory, the hacktivist group tried to cripple Israeli sites and government networks.

The move came as Israel admitted the war is being fought on 'three fronts' - including physical, social networks and cyber attacks - and triggered calls for a 'cyberdome' protective shield to mirror the 'iron dome' missile defence system.