Practical Security and Key Management

University of Amsterdam
SNE - Research Project 2

By:
Magiel van der Meer

Supervisors:
Marc Smeets
Jeroen van der Ham

July 2, 2014

Introduction

- Encryption and authenticity more important
- Personal data over untrusted networks
- .. thus for eavesdropping

- Truly secure communications are non-trivial (if not impossible)
- Lots of information available on Internet, but..
- .. not necessarily up-to-date
- .. not always supported with facts
- .. might be plain wrong

Research Question

Research Question

How can one combine practical security and secure key management by aggregating relevant public available information?

Points of interest

- Security levels
- Elements to secure
- Best practices per level and element
- Practical configurations for elements
- Overview guide

Security levels

Defined security levels

- Basic
- Medium
- High

Security levels

Basic

Basic

- e.g. Individual security enthusiasts
- e.g. OS3 Students
- Signing / encrypting e-mail
- e.g. Web shops working with privacy sensitive customer data
- Securing connections from customer to web shop
- Likely no budget or related hardware

Security levels

Medium

Medium

- e.g. Journalists in countries with repressive regimes
- e.g. IT security researchers
- Signing / encrypting e-mail
- Securing the workstation
- e.g. Banks processing customer payments (Online banking)
- Probably budget & related hardware available

Security levels

High

High

- e.g. Employers of corporations (Banks, R&D sensitive)
- e.g. IT security researchers
- e.g. Separate private key operations from production machines
- e.g. Predefined procedures for certificate issuance and revocation
- Desire for centralized key management
- Budget & specialized hardware available (like HSM)

Secure elements

Elements to secure

- Key management
- Personal communications
- System communications

Secure elements

Personal communications

Personal communications

- Securing digital communications between humans
- End-user involvement required

- Pretty Good Privacy (PGP)
- S/MIME
- Off-The-Record (OTR)

Secure elements

System communications

System communications

- System to system security
- Operations mostly transparent to the end-user
- Only involve (or not ..) end-user when security fails

- Web, mail, remote management, .. (Secured versions of course)
- All these have in common: TLS/SSL

Key management

Considerations

Key management

- Backup
- Escrow
- Recoverability historic data
- Logical access
- Physical access
- Revocation procedures
- Decrypt and encrypt data when new key is issued
- Use key only on secure environment

Overview

Cross reference Security levels (Header) with the defined Secure elements (1th column)

What?	Basic	Medium	High
Personal security	Best practices & corresponding configurations per level		
Key management			
System communications			

Pretty Good Privacy
Considerations

PGP concepts

- Generation of keys
- Key storage
- Key lengths
- Role separation
- Expiration
- Publishing
- Rollovers
- Revocation
- Web-of-trust

HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:
LOOK FOR THIS TEXT AT THE TOP.
REPLY
-----BEGIN PGP SIGNED MESSAGE-----
HASH: SHA256
HEY,
IF IT'S THERE, THE EMAIL IS PROBABLY FINE.

Figure : Randall Munroe (xkcd)

Transport Layer Security

Considerations

Cryptographic protocol

- Key agreement or establishment
- Peer authentication
- Symmetric encryption and authentication
- Secure data transport
- Non-repudiation

Transport Layer Security

Asymmetric & symmetric

- Asymmetric operations are expensive
- Uses asymmetric cryptography
- To authenticate and exchange symmetric key for encryption of data

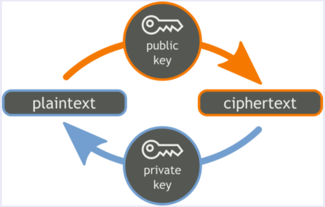

Figure : Corredera Jorge

Findings

Key management

What?	Basic	Medium	High
Key generation	(Offline live) system	Offline live system Yubikey/Smartcard	Specialized hardware Personal tokens
Backup	Would be very smart	Should be done	
Escrow	Depends on the situation		
Revocation procedures	Signed mail to known contacts		Planned procedure
Key usage	Only in trusted environment		

Argumentation & sources in paper

Findings

PGP

What?	Basic	Medium	High
RSA/DSA-Elgemal	RSA		
Role separation	Default		Subkey for certification
Length (Bits)	2048	4096	S:4096 M:8192
Expiration	Subkey: 1y / Masterkey: 2y		
Revocation	Mandatory, but implementation may differ		
Rollover	Signed mail to known contacts		Planned procedure

More argumentation & sources in paper

Findings

System communications

Considerations

- Choices depend more on target end-users / clients than security levels
- Self-signed certificate or well-known CA[1]
- Public (web) service should support range of cipher suites
- Mail server with managed clients can be more strict

[1] Certificate Authority

Conclusion

A lot of information available

- Often incomplete and no background or sources
- Spread over numerous sources (Blog entries, NIST recommendations,..)
- Out of date information (GnuPG manual: Go for 1024 bit DSA key)
- Corporate advisories (Microsoft, RSA,..)
- Can't see the Wood for the Trees

Now even more information

- But complete
- Background information
- Argumentations and sources given
- Applicable to several environments (security levels)
- A little bit more light in the darkness

Questions?

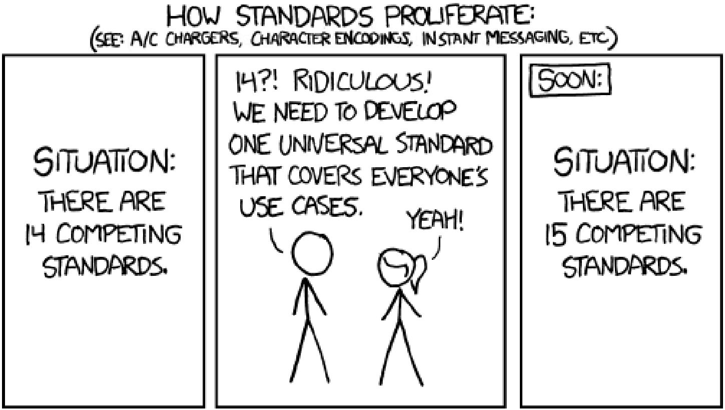
HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Figure : Randall Munroe (xkcd)