Simplicity Arriving Too Late to Save a Drowning PKI?

Werner Koch

2010-11-11 Thu

Outline

PK Intro

PKI Technik

Probleme

Lösungen

Infos

Public-Key Kryptographie

- Öffentlicher Teil zum Verschlüsseln und zur Prüfung von Signaturen
- Geheimgehaltener Teil zum Entschlüsseln und Signieren
- Bekannte Algorithmen: RSA, DSA, Elgamal, ECC

Schlüsselverteilung

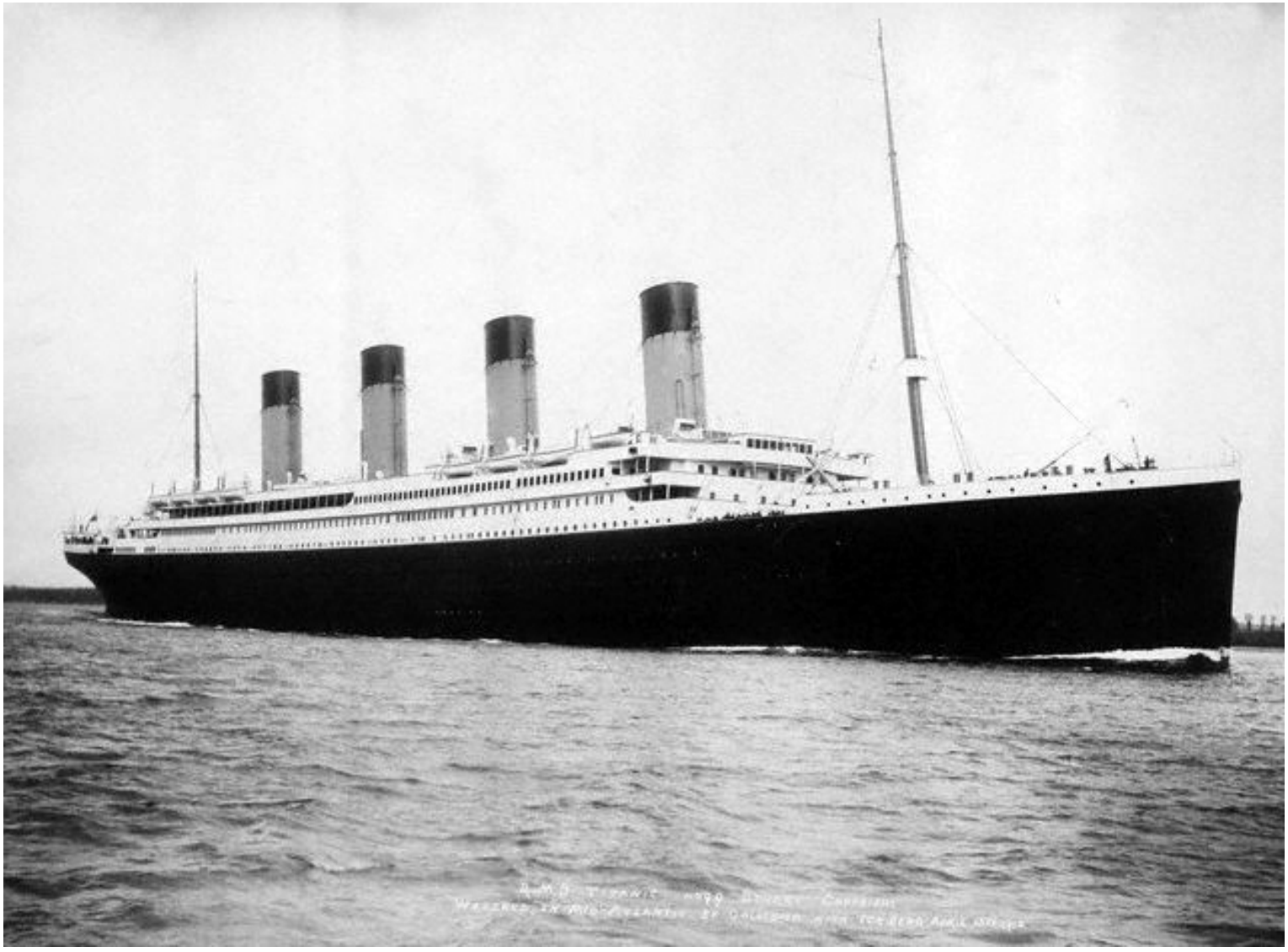
- Individuell
  - per Email
  - per Diskette etc.
- Über bekannte Webadressen
  - Speichern des Keys auf der Kontaktseite
  - Beispiele: CERTs, Datenschutzzentrum
- Über zentrale Server
  - Das Netz der OpenPGP Keyserver
    Vorteil: syncronisiert
  - LDAP Server
    Nachteile: Unkoordiniert; viele individuelle Server

Wozu dienen PKIs

- Verteilen der Schlüssel
- Aufdecken und Verhindern von MitM Angriffen
- Widerrufsverwaltung

Wozu dienen PKIs wirklich

- Geschäftsmodell der Serversteuer



X.509: Die göttliche Idee — Kritik nicht erwünscht

Designed by Committee

- In den 80er Jahren von der ITU als Authentifizierungsverfahren für das X.500 Verzeichnis entwickelt
- Basiert auf einem streng hierarchischen System mit nur einer Wurzel
- X.500 wurde niemals wirklich realisiert
- X.509 hat in verschiedenen Ausprägungen überlebt aber mit vielen Wurzelinstanzen

PGP: Hilfe für Graswurzelbewegungen

Ad-hoc Lösung

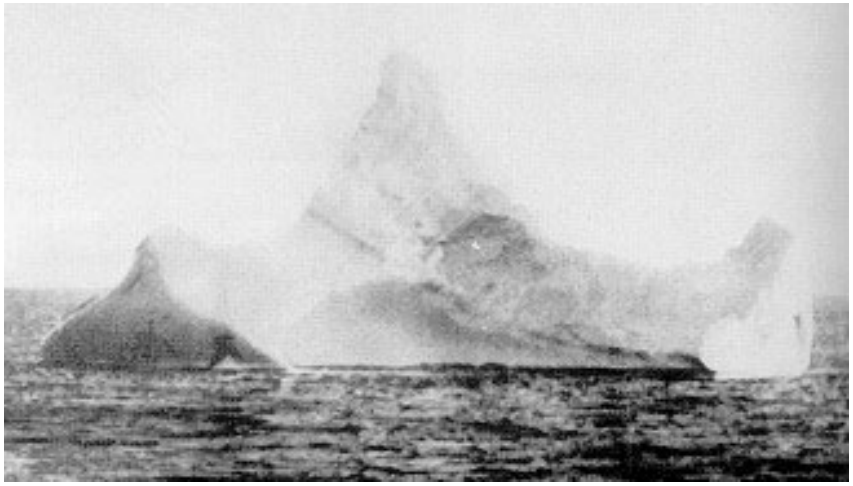
- Web-of-Trust (WoT) als Vertrauensmodell von PGP 2.
- Dezentraler Ansatz
- Funktionsfähig ohne direkte Kosten und ohne zentrale Verwaltung
- Weit verbreitet unter Technikern

Das WoT reflektierte am besten die Wirklichkeit der Kommunikation vor ~10 Jahren.

OpenPGP: Wir können PGP und alles andere auch

IETF Kompromiss

- Basiert auf PGP 2
- Erweitert um nützliche Features
- Erweitert um Features für eine X.509 Architektur
- Der Standard beschreibt nur Features aber kein PKI



Die Standards

Das Schöne an Standards ist, daß jeder sich seinen eigenen aussuchen kann.

Der X.509 Standard

You can't be a real country unless you have a beer and an airline. It helps if you have some kind of a football team, or some nuclear weapons, but at the very least you need a beer.

– Frank Zappa

And an X.509 profile.

– Peter Gutmann

- Profile in allen möglichen Varianten und Mischungen
- X.509 benutzt ASN.1 basierte Kodierungen

Der OpenPGP Standard

- OpenPGP hat einen eindeutigen Standard
- Basiert auf dem IETF Konsens
- Implementierungen wurden mit dem Standard entwickelt
- Gegenseitige Tests

Auffinden von Schlüsseln

- X.509
  - X.500 sollte es regeln — gibt es aber nicht
  - LDAP Server — nur welcher
  - Es gibt im LDAP keinen Standard wo die Zertifikate gespeichert sind
- OpenPGP
  - De-facto Standard: SKS Keyserver (z.B. keys.gnupg.net)
  - ASCII Armor für Webseiten
  - OpenPGP Mail Header als Referenz

Die Kosten

- Schulungen für Admins
- Zertifikate laufen ab und müßen neu beschafft werden
- Webshops arbeiten nicht, da das Zertifikat abgelaufen ist
- CRLs sind nicht erreichbar
- Hohe indirekte Kosten wg. schlechter Verfügbarkeit

X.509 Realität

Laut dem EFF SSL Obervatory (Defcon 18, 2010):

- 1482 CA Zertifikate in Windows oder Firefox
- 641 Organisationen
- Alleine 300.000 Server Zertifikate von GoDaddy
- 192.168.1.2 z.B. von Equifax zertifiziert
- Mehr als 6000 Zertifikate für “localhost”
- Hunderte von Sub-CAs zertifiziert.

OpenPGP Realität

Funktioniert leidlich, da

- kaum technische Probleme
- gegenseitige Hilfe üblich ist
- das WoT meist ignoriert wird

Die Wartbarkeit

Oh je.

Die vermeintliche Sicherheit

- **Der Standard**: Warnungen werden ignoriert.
- Ein Aufschrei sobald das Ignorieren von Warnungen schwieriger gemacht wird
- Crypto MiTM sind mehr als selten, da nicht notwendig
- Wichtiges Maßnahme z.Z.: 2048 Bit Keys:

  Formal notice given of rearrangement of deck chairs on RMS PKItanic

Das Verständniss

- Benutzername + Passwort sind halbwegs verständlich
- Erklärung von Zertifikatsketten?
- CRL erklären?
- Warum Schlüsselauswahl?

Das User Interface

- PKIs sind ein realitätsfernes System
- Entspricht nicht dem Benutzerverhalten
- Spiegelt nicht die Struktur des Netzes wieder

Sind Lösungen noch möglich?

- Eine radikale Vereinfachung ist gefragt
- Die PKI sollte der Struktur des Netzes entsprechen
- Warnmeldungen so selten wie möglich und mit Handlungsanweisungen

1. Versuch (PKA)

Public-Key-Association

- Idee: Identitäten (Fingerprints) an das DNS binden.
- Sicherheit liegt allein im DNS
- Vorhandene und sehr gut skalierende Infrastuktur
- Einfaches Auffinden von Schlüsseln
- Seit vielen Jahren in GnuPG vorhanden

2. Versuch (SSH)

Secure Shell - Admins Liebling

- Die einfachste PKI die vorstellbar ist
- Auch ohne Vergleich der Host-Keys relativ sicher
- Änderung des Host-Keys bewirkt deutliche Warnung
- Leicht zu verstehen

Was nun?

- Selbstsignierte X.509 Zertifikate
- Standard OpenPGP Keys und Option –always-trust
- Das SSH Modell wird benutzt
- Design eines sehr guten UI für den Fehlerfall

Was nun? (lynx)

- Webbrowser
  - Speichern: Domainname, Fingerprint
  - Keine Prüfung der Zertifikatskette
  - Warnung falls gespeicherter Fingerprint nicht mehr übereinstimmt

Was nun? (mail)

- Email etc.
  - Speichern: Absendername, Fingerprint
  - Normale Prüfung
  - Signatur gültig wenn Absendername + Fingerprint übereinstimmen.

Was nun? (/etc)

- Andere Anwendungen
  - Software muss i.d.R. öfter erneuert werden als Zertifikate
  - Signaturprüfung mit eingebettetem Zertifikat
  - Zertifikat im Binary oder Extradatei
- Spezielle Lösungen für Online Banking etc.
  - Apps müssen nicht nur für iFoos sein.

Was muss gemacht werden?

- UI Design
- Plugins für Firefox und Internet Exploder
- Mailer anpasssen
- Wie kann GnuPG helfen?
  - Neues Trustmodeel (ala PKA)
  - Datenbank für Mail Adressen und Schlüssel
  - Kontakthistorie (letzte 5 Kontakte)
  - Neue Flags und Calls in GPGME um dies zu representieren

URLs

- PKA Beschreibung:
  ftp://ftp.g10code.com/people/werner/talks/pka-intro.ps.gz
- X.509 Style Guide:
  http://www.cs.auckland.ac.nz/p̃gut001/pubs/x509guide.txt
- EFF SSL Observatory:
  https://www.eff.org/observatory