A New Cryptographic Technique with Applications to Mobile Security

Pomcor

http://pomcor.com/
Outline

- Security challenges of mobile devices (smart phones, tablets)
- New technique: RSA key pair regeneration
- Application to user authentication
- Application to data protection
- Strategic benefits
- For more information…
- About Pomcor
Security Challenges of Mobile Devices

- **User authentication**
  - Difficult to enter high entropy passwords (long passwords with letters, digits and other characters)
  - One-time passwords (OTP) are cumbersome and fail to provide strong security

- **Data protection**
  - iPhone hardware encryption fails to protect data in device that has been lost or stolen
New Technique: RSA Key Pair Regeneration

- Store prime factors of RSA modulus
- Derive private key from PIN or biometric key
- Compute public key from private key and prime factors
- For more details, see our presentation to the Cryptographic Key Management Workshop at the National Institute of Standards and Technology (NIST)
- Crucial benefit: immunity to offline attack
Application: Two-Factor Cryptographic Authentication

- User enters PIN
- Mobile device regenerates key pair and uses it to authenticate to app back-end
- App back-end verifies that hash of public key is present in database record created for mobile device
- Device record refers to user record
Key pair regeneration

PIN

Public key

Proof of knowledge of private key

Hash function

Database

User record

Device record

Hash of public key

User record

Database

Hash function
Three-factor Cryptographic and Biometric Authentication

- We intend to use an iris biometric sample taken by the mobile device front camera
  - Following prior work by Hao, Anderson & Daugman (0.47% false rejection rate, 0% false acceptance rate)
  - No biometric feature template stored in device, as prescribed by ISO 24745 Biometric Information Protection
- Biometric key consistently derived from genuine biometric sample and auxiliary data
- Biometric key used to regenerate key pair
- PIN used to encrypt auxiliary data
Key pair regeneration

Bio key generation

Bio key

Aux. data

Encrypted aux. data

PIN

Iris image

Proof of knowledge of private key

Hash function

Database

User record

Device record

Hash of public key
Encapsulation of Cryptographic and Biometric Software

- Prover Black Box (PBB) in mobile device
  - Obtains PIN and optional iris image, regenerates key pair
- Verifier Black Box (VBB) online
  - Verifies proof of knowledge of private key
- App developer does not have to know cryptography or biometrics

- Many configurations options
  - PBB: in OS / in app / separate app / browser plug-in
  - VBB: in app back-end / server appliance / trusted 3rd party
Authentication Use Cases

- Employee authentication in enterprise
- Consumer authentication
  - PBB contains multiple credentials for multiple apps
- Social login without a password
  - VBB in social network provides access token to app
- Derived credentials for US federal agencies
  - See NIST workshop presentation
- Citizen credentials in countries other than US
  - Credential created by device and registered with same agency that issues the national ID card
The Data Protection Challenge

Problem: how to protect data stored in mobile device that is lost or stolen

- Encrypt data?
  - Not secure if data encryption key is stored in device without tamper protection
- Data encryption key derived from PIN?
  - Not secure because PIN is vulnerable to offline attack
- Hardware key + PIN, as in iPhone?
  - Not secure because custom code can use the hardware key to crack the passcode
- Our key pair regeneration technique provides a solution
Solution

- Encryption key stored in trusted server, or split over multiple servers with $k$-of-$n$ Shamir secret sharing
  - User enters PIN or PIN + iris image
  - Mobile device regenerates key pair and uses it to authenticate to server(s)
  - Server(s) provide(s) data encryption key over secure connection(s)
- Server(s) could be provided by
  - Mobile network operator, or
  - OS provider (e.g. Google), or
  - Mobile device manufacturer, or
  - Ad-hoc data protection service trusted by user
Strategic Benefits

- Secure cryptographic two- or three-factor authentication without asking user to provide high entropy password or one-time password
- Social login without a password
- Effective data protection if device is lost or stolen
- No need for tamper resistant module or hardware encryption chip
- Developers don’t need to know cryptography or biometrics
- Several patents pending
  - Pomcor’s CTO is a proven inventor with 9 patents granted
For More Information

- Pomcor web site: [http://pomcor.com/](http://pomcor.com/)
- Pomcor blog: [http://pomcor.com/blog/](http://pomcor.com/blog/)
- White papers:
  - Effective Data Protection for Mobile Devices
  - Techniques for Implementing Derived Credentials
  - Strong and Convenient Multi-Factor Authentication on Mobile Devices
- Presentation to NIST workshop on Cryptographic Key Management:
  - Key Management Challenges of Derived Credentials and Techniques for Addressing Them
- Contact us:
  - fcorella@pomcor.com
  - kplewison@pomcor.com
Pomcor is an independent research and development company working on several areas of web and mobile technology, including security, cryptography, collaboration and search. Pomcor’s mission is to identify shortcomings of current technology and provide innovative solutions that advance the state of the art. It has received an NSF grant and been invited to participate in several NIST and W3C workshops.

Pomcor has invented methods of protecting passwords against online-guessing attacks, securing the distribution of temporary passwords, protecting file-sharing applications against attacks through shared files, using cryptography and biometrics to authenticate users of mobile devices; and, in the area of search, methods of exploring the result sets of multiple queries simultaneously, analyzing queries that produce zero results, and browsing real-time results that change as they are being browsed. It has created Noflail Search, a multisearch engine available at noflail.com that incorporates several of the search innovations.

Pomcor was funded by Karen Lewison, MD, who provided initial financing and is currently CEO, and Francisco Corella, PhD, who is currently CTO. Dr. Corella is a graduate of the Ecole des Mines de Paris, Stanford University, and the University of Cambridge. He has broad experience in the computer industry, having worked as a manager at Symantec, as a researcher at Schlumberger Palo Alto Research and the IBM T.J. Watson Research Center, and as an engineering-scientist at the Unix laboratories of HP. He is an inventor with 9 patents granted. Pomcor’s Advisory Board includes Marc Friedmann and Gary Pritchett, Entrepreneurs –In-Residence at CONNECT in San Diego. Marc Friedmann is an experienced CEO and currently a partner at DaggerBoard Advisors. Gary Pritchett has over 30 years of experience as software development executive and is currently COO of Terra Knights Music, Inc.