JavaOne℠

Sun's Worldwide Java Developer Conference

Sun's World Wide Java Developer Conference

Trust, Proof, and Payment

Software Distribution in the Age of the Internet

Scott Schnell

RSA Data Security, Inc.

Security and Java

- Current focus on boundaries and detecting “bad” applets at runtime
  - Distinguishing “trusted” from “untrusted”
  - Limiting applet activity
  - Severely limiting “untrusted” applet activity
- Current applet screening very coarse
  - Netscape - local vs remote
  - Others - inside/outside firewall, etc.
- Where is user judgment?

What Do the Players Want?

- Users want control in:
  - Trusting the author and integrity of the applet
  - Authenticating the “reseller” of the applet
  - Preventing fraudulent use of their credit cards
- Developers want:
  - Payment
  - Piracy prevention
- Electronic distributors and resellers want payment and info
- Visa and Mastercard want to prevent fraud

...all before the applet is loaded

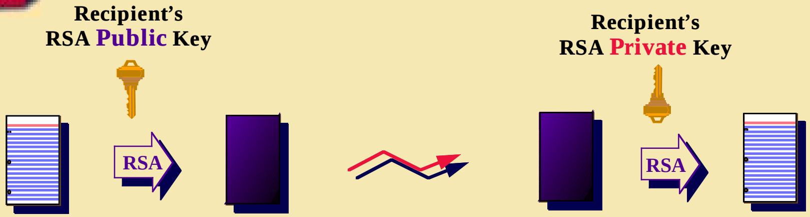
Security Foundation for Applet Sales and Distribution

- SSL
  - Secure piping
- Signed applets and signature-aware browsers
  - Integrity of application
  - Authenticity of developer
  - User decides which ***developers*** she trusts!
- Secure transactions (SET)
  - Authentication — Cardholder, Merchant, and Acquirer
  - Protection of CC information
  - Indemnity — for merchant and cardholder
  - Fraud Control — for issuers
- Signed distribution
  - Trusted reporting of distribution chain back to developer

RSA Crypto Foundation

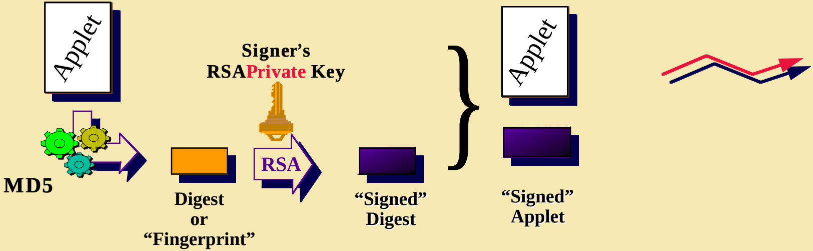
- RSA Digital Signature
  - Authenticates author and integrity of a document or application
- RSA Digital Envelope
  - Provides privacy for communication, transactions, and data between sender and recipient
- Both based on RSA Public Key Cryptography and Digital Certification of keys

Public Key Crypto Basics



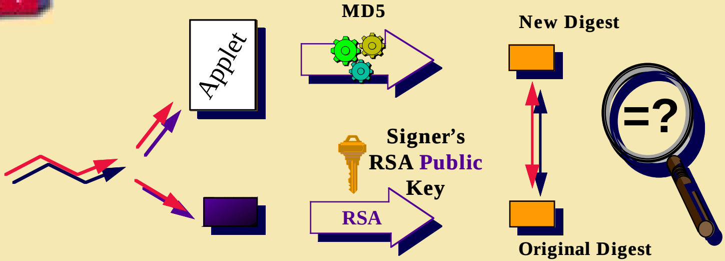
- Algorithm asymmetrical
  - Pair of keys for each entity
  - What the Public key locks, only the Private key unlocks, and vice versa
- Eliminates need to share secrets
- Allows positive identification of sender and recipient

Signing an Applet

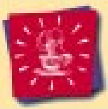


- Author Signs a “fingerprint” of the Applet and binds it to the Applet

Verifying a Signature



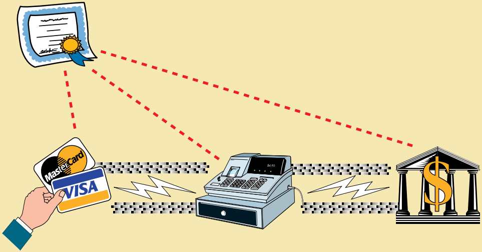
- Recipient decrypts original fingerprint, and matches it with a new one
  - Verifies both integrity of applet and author's identity



Certificates

- You need to have trust in the “labeling” of public keys
- Certificates establish trust indirectly via trusted “Certificate Authorities” — i.e., Verisign
- Uniform mechanism
- Many certificates for many purposes
- Facilitates secure, *ad hoc* commerce and communication

SET — the Secure Payment Card Transaction Standard



- "Preflights" the identity of all participants using certs and challenges
- Obscures Credit Card from merchant until after identities and approval are complete
- Deals only with value and method of transaction, not the order
  - Restrictions make it strong and exportable worldwide

What’s Next

- Java standards for code signing using digital signatures
- Java browsers that check applet signatures and inform the user
- Certificate standard and infrastructure for signature verification
- SET finalization and deployment in browsers, merchant servers, and payment gateways

Contacting RSA

- http://www.rsa.com
- info@rsa.com
- RSA-labs@rsa.com

RSA Data Security, Inc.
100 Marine Parkway, Suite 500
Redwood City, CA 94065
415 / 595-8782 vox
415 / 595-1873 fax

JavaOne℠

Sun's Worldwide Java Developer Conference