Visualizing Your Key for Secure Phone Calls and Language Independence

Michael Oehler, Dhananjay Phatak, John Krautheim
University of Maryland Baltimore County
Baltimore, Maryland USA

VIZSEC, 14 SEP 2010, Ottawa Ontario, Canada
Objective

- Problem Area
- Approach
- Discussion
Problem Area

• Providing Security for Internet Protocols
  – Internet Phone Calls
    • Voice Over IP (VoIP) Security
      – SIP, SDP, RTP, DNS
    • Other secure voice/video systems

• Involve the user in the “security process”
Problem Area

- Passive
  - Eavesdropping

- Active Attacks
  - Flooding, VoIP Spam, Call Hijacking
  - MITM

- Implementation and Configuration Errors
  - Intentional and Unintentional
    - Leads to VoIP specific attacks
Problem Area

• To protect the media, the call requires
  • Confidentiality
    – Key negotiation
      » Authentication
Problem Area

- Security as seen by the user
  - SSH
    - First Time: Blindly accept?
      unix:~/.ssh mjo$ ssh -l mjo 192.168.1.3
      The authenticity of host '192.168.1.3 (192.168.1.3)' can't be established.
      Are you sure you want to continue connecting
      Yes/No?
  - Web of Trust
  - HTTPS
    - PKI
Approach

- How to Engage the user in security process?
  - Effective Mechanism
    - Based strong cryptography
  - Simple Mechanism
    - Without intricate knowledge of cryptography
    - Useful to all
Approach

• Securely derive a session key
  – Utilize a Key Management Protocol

• Derive visual encoding of the Secret key
  – Present an image on both systems

• The users then verbally confirm what they see
  – You recognize the caller’s voice
  – You trust the caller
Approach

• Present a visual interface component
  • Basic geometric shapes, color, and count
Approach

• Easily Identifiable
  – Color, count, and shape
• Independent of Language

• Lightweight Security Mechanism

• Applicable for caller’s social network
  – Friends, family, colleagues
Approach

- 2 Sets of shapes, 4 Colors, 8 Arrangements

- Glyph for every byte
Discussion

• Side Channel Authentication
  – A mechanism and/or medium providing Authentication
    • That is not readily accessible to the adversary
      – And thus, not easily forged.
  – Mechanism
    • Art → PKI Certificate Representation,
    • Bar Code → Public Key
    • 3-Dimension Scene → Internet Transaction
  – Medium:
    • Visual, audio, Out-of-Band data network
Discussion

- AT&T TSD 3600, 1993
  - Read some bytes

- PGPfone, 1996

- ZRTP, 2010
  - Phil Zimmermann Real Time Protocol
  - “Short Authentication String”
  - English Only

- Engage all users!
  - Leverage visualization
Discussion
Select Glyph from Alternate Sets

SHA(key) = \langle v_n, \ldots, v_3, v_2, v_1, v_0 \rangle

\text{Image} = \langle g_{Odd,v_3}, g_{Even,v_2}, g_{Odd,v_1}, g_{Even,v_0} \rangle
Discussion

Alice

Pick $d_A$
Compute $A = d_A(G)$
Compute $H(A)$

$H'(B) = H(B)$
Create Key:
$K_{AB} = d_A(B)$

The Image hash
$V_{AB} = H(K_{AB})$

Bob

Pick $d_B$
Compute $B = d_B(G)$
Compute $H(B)$

$H'(A) = H(A)$
Create Key:
$K_{AB} = d_B(A)$

The Image hash
$V_{AB} = H(K_{AB})$

Send Commitment
Send Public
Encrypted Channel
Describe Image
Discussion

• Prototype
  – Scaleable Vector Graphic (SVG)
    • Represent all combinations of images
    • Small Footprint

<desc>Two Red Square</desc>
<g transform="translate(16,8)">
<svg width="56px" height="56px">
<rect x='10' y='10' width='200' height='200' fill='Red' stroke='black' stroke-width='2' />
</svg>
</g>
...
Discussion

• Observations
  – People “Get It”
  – Saw the rouse
  – Will they use?
  – Color Blind.
Thanks

- Michael.oehler@umbc.edu