W3Bcrypt: Encryption as a Stylesheet

Angelos Stavrou
and
Michael E. Locasto

Columbia University
Motivation

- Current Trust Model == New Threat Model
  - Communications infrastructure provider
  - Third party hosting of communication and commerce
  - Gmail

- Security Threats
  - Confidentiality
  - Integrity
  - NOT availability
Current Approaches

- Confidentiality and integrity for web communications
  - IPsec (layer 3, threat is trusted network insider)
  - TLS/SSL (layer 4, threat is OS)
  - HTTPS (application layer, threat is server app)

- No protection for presentation-level content objects (i.e., HTML elements) from the server
Key Insights

- Use communications provider as a transit conduit
  - public-key, E2E cryptography
  - PGP

- Cryptographic operations are a style
  - applied to web content along with layout, etc.
  - automatically applied

- Create trusted environment within the browser
  - extend the browser – local environment
  - can't trust code from the server (Javascript, etc.)
Use Cases

- (peer) Webmail client with PGP
- (customer) Customer of online merchant
  - communicate with financial institution
- (publisher) Content publisher
  - news service
  - blogger
  - digital media
Operation: Webmail Case

- Cannot trust Java Applet, ActiveX, or Javascript code for PGP
  - delivered from the server
  - sharing private key with the server!
  - code signing/proof-carrying code a maybe

- Need independent, client-side PGP environment in the browser
Webmail Send
Webmail Send (cont)
Operation: Auto Rendering

- When DOM finishes loading
  - grab list of `<div>` elements
  - see which are marked with class of “w3bcrypt”

- Pass content to GPG
  - decrypt
  - re-insert into HTML content
  - Firefox renders decrypted content
Implementation

- Firefox 1.5.x extension
  - GUI overlay + Javascript functionality
  - Unix/BSD/Linux (xterm)
  - GnuPG
- Context-menu
  - PGP operations
    - encrypt, sign, sign/encrypt
    - decrypt, verify, decrypt/verify
- Auto-decrypt of `<div>` elements
  - other tags?
Evaluation

- Attacks
  - recall threat model

- Performance
  - Time for cryptographic operations
  - Extra storage space required
    - binary
    - text
Attacks

- DoS, Brute force on PGP
  - non-availability is not productive for service provider
  - unlikely & not our problem

- Hitchhiker
  - Server sends Javascript that monitors
    - input (Gmail spell-checker)
    - output (read page after it is decrypted)
  - Phishing (server inserts content)
    - defeat with signed content

- Replay
  - append time-stamp or sequence number
Time Measurement

Encryption & Decryption times for Text

<table>
<thead>
<tr>
<th>Plaintext Size (in Bytes)</th>
<th>Enc 4,143</th>
<th>Dec</th>
<th>Enc 9,005</th>
<th>Dec</th>
<th>Enc 25,718</th>
<th>Dec</th>
<th>Enc 38,336</th>
<th>Dec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time (in seconds)</td>
<td>0.05</td>
<td>0.04</td>
<td>0.05</td>
<td>0.04</td>
<td>0.06</td>
<td>0.05</td>
<td>0.06</td>
<td>0.05</td>
</tr>
</tbody>
</table>
Content Sizes

**Graph:**
- **Title:** Encrypted/Plaintext ratio for various sizes of text
- **Y-axis:** Encrypted/Plaintext (0% to 140%)
- **X-axis:** Plaintext Size (in Bytes) [4,143 to 38,336]

The graph shows the increase in size from plaintext to ciphertext as the plaintext size increases.

**Legend:**
- Each bar represents a different plaintext size, with the bar height indicating the encrypted size relative to the plaintext size.
Website Sizes

Size Comparison for Web Content

<table>
<thead>
<tr>
<th>Size (KBytes)</th>
<th>CNN.com</th>
<th>CNN.com Encrypted</th>
<th>CNN.com</th>
<th>CNN.com Encrypted</th>
<th>Chase.com</th>
<th>Chase.com Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>600K</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>500K</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>400K</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>300K</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>200K</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100K</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- Images
- HTML and Javascript
Benefits

- Mostly transparent privacy-enhancing browser extension
  - trusted environment within the browser
  - not server-delivered Javascript!
  - browser-as-OS-platform model
- Offload cryptographic (e.g., SSL) processing from the server to the client
- Concept of cryptographic processing as another phase of styling web content
Conclusion

Future
- address Hitchhiker attack (implement countermeasure)
- add timestamp option to fields
- help with trusted path problem/visual phishing
- key management

Need developers/testers
- for Windows
- for other PGP packages on host
- bundling or download of GnuPG
Contact

http://nsl.cs.columbia.edu/projects/w3bcrypt
BACKUP SLIDES