June 17-19, 2014 | Cobb Galleria | Atlanta, Georgia

WebRTC IV
CONFERENCE & EXPO

The Longest Running Global WebRTC Ecosystem Event

#webrtcexpo | @webrtcexpo

www.webrtcexpo.com
Security Considerations for Service Providers

Rich Tehrani
TMC
Speakers

• Glen Gerhard
  – Sansay

• Justin Hart
  – Sonus
Glen Gerhard
Sansay
Why worry?

• Two thirds of large organizations report a DDOS attack last year, 11% had more than 6 attacks
• Same organizations report 33% network downtime is due to DDOS attacks
• Target, eBay, Twitter, Facebook, Evernote, etc leaks
• 2011 carrier losses: $4.9B to compromised PBXs
  – $ 4.3B due to identity/subscription theft
Security is key enabler

• More attack surfaces than POTS so greater risks
• Greater risks mean greater rewards for attackers
  – More at stake than a SIP phone (Heartbleed, Malware, POS)
# Attack surfaces/ownership

<table>
<thead>
<tr>
<th>APPLICATION LAYER</th>
<th>CLIENT/USER</th>
<th>SERVICE PROVIDERS</th>
</tr>
</thead>
</table>
| **Proper browser/Java versions** | Server Availability | Application DB security
|                             | Proper Routing and Presence                     |
| **ISP and local links**    | ISP/BGP service at colos                       |
| **Firewalls and routers**  | Cloud systems and management                   |
| **DNS servers**            | Media relay points                             |
| **Anti-virus software**    | Properly designed scripts                       |
| **Operating system**       |                                                 |
| **DNS settings**           |                                                 |
| **User Authentication security** |                                              |
# Attack Goals and Counters

<table>
<thead>
<tr>
<th>USER SURFACE</th>
<th>COUNTERMEASURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implant malware</td>
<td>Sandbox certain aspects of application such as file sharing. Ask for file save location.</td>
</tr>
<tr>
<td>Steal User Data</td>
<td>Limit usage of Contact or other list in the client devices.</td>
</tr>
<tr>
<td>Camera jacking</td>
<td>Observe user authorizations and notifications.</td>
</tr>
<tr>
<td>Monitoring session media</td>
<td>Provide full encryption for all traffic.</td>
</tr>
<tr>
<td>Theft of service (via authentication)</td>
<td>Monitor usage for toll fraud with advanced heuristic analysis.</td>
</tr>
</tbody>
</table>
## Attack Goals and Counters

<table>
<thead>
<tr>
<th>NETWORK SURFACE</th>
<th>COUNTERMEASURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDOS User site</td>
<td>Direct or MPLS to customer site. Redundant local loops.</td>
</tr>
<tr>
<td>DDOS Service Provider Site</td>
<td>Have redundant sites with large redundant BGP pipes. Create response protocols with ISPs to block attacking ASNs. Use offload/scrubbing service.</td>
</tr>
<tr>
<td>Media layer DOS attacks</td>
<td>Use many private TURN servers or SBC alternatives. Use offload/scrubbing service.</td>
</tr>
<tr>
<td>Monitoring session media</td>
<td>Provide full encryption for all traffic.</td>
</tr>
<tr>
<td>Network edge penetration attack</td>
<td>Advanced firewalls with DPI. Monitor devices for usage stats.</td>
</tr>
</tbody>
</table>
## Attack Goals and Counters

<table>
<thead>
<tr>
<th>APPLICATION SURFACE</th>
<th>COUNTERMEASURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDOS attack</td>
<td>Have redundant sites with large redundant BGP pipes. Create response protocols with ISPs to block attacking ASNs. Use offload/scrubbing service.</td>
</tr>
<tr>
<td>Steal User Data</td>
<td>Keep system authorizing uses at latest levels for all processes. Only allow relevant ports open to those systems.</td>
</tr>
<tr>
<td>Penetration attack on servers.</td>
<td>Only allow relevant ports to be accessed. Monitor syslog or events for access attempts. Advanced firewalls for DPI alerting.</td>
</tr>
<tr>
<td>Theft of service (via authentication)</td>
<td>Monitor usage for toll fraud with advanced heuristic analysis.</td>
</tr>
</tbody>
</table>
Justin Hart
Sonus
Security is More than just Encryption

- Authentication
  - Nothing specific in WebRTC
  - Leverage existing web mechanisms
  - Other mechanisms?

- Authorisation
  - Mic/Camera Controls
  - Most everything else is application specific

WebRTC is good:
- HTTPS
- DTLS
- SRTP-DTLS

Encryption

Session
WebRTC Use Cases & Authentication Options

- **Web**
  - OAuth2.0
  - OpenID

- **Enterprise**
  - LDAP
  - Active Directory
  - PBX
  - SIP Registrar

- **3GPP**
  - SIP Registrar
  - IMS core

- **Custom solutions**
Authentication using Web ID

Customer

Carrier

Identity Provider

WebRTC GW

Policy DB

SBC

TURN Server
Authentication using Enterprise ID

<table>
<thead>
<tr>
<th>Customer</th>
<th>Carrier</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Hosted UC
- WebRTC GW
- Policy DB
- SBC
- TURN Server
Breeds Different User ID Domains

Customer | Carrier
---|---
Identity Provider | Hosted UC

WebRTC GW | Policy DB

SBC

IMS Core / PSTN

TURN Server

www.webrtcexpo.com
WebRTC Access to IMS Services
WebRTC Access to IMS Services

Securing the Media

WebRTC
IMS Client

Providing Web Signalling and control

Securing & Working Signalling

WebRTC Working Group

Sonus
User Registration based on Web Identity

1. HTTPS to web server, returning auth grant assertion
2. Open secure WebSocket using CORS
3. REGISTER request with assertion
4. OK response
5. SIP REGISTER

WWSF is charged with querying some (unspecified) external DB to get IMS identities.

eP-CSCF forwards to IMS core with indication that authentication has already occurred.
User Authentication using IMS Identity

1. HTTPS to web server
2. Open secure WebSocket using CORS
3. REGISTER request
4. Unauthorized response
5. REGISTER request
6. OK response

UE obtains IMS registration details by unspecified means (e.g. cookie)

Registration Procedures follow normal IMS steps
In Conclusion

- WebRTC provides a lot of good security building blocks
- WebRTC diverse use cases foster diverse identify & authentication schemes
- Thought needed about how to combine into end-to-end security approach
  - How do you want to identify your users and bring them into your network?

Get free WebRTC dummies guide here
http://info.sonus.net/webrtc-dummies-snet-new
Thank You

Please remember to complete an evaluation of today’s sessions
Questions (hidden)