RTC-Web Framework

Jonathan Rosenberg
Chief Technology Strategist, Skype
Base Case (Model 1)

Application Provider

Proprietary Over HTTP/Websocket

JS/HTML App

JS API

JS/HTML App

Browser

Media + Media Path Signaling (ICE/STUN/TURN)
Base Case (Model 2)

Application Provider

Standardized Signaling

JS/HTML App

JS/HTML App

JS API

Browser

Browser

Media + Media Path Signaling (ICE/STUN/TURN)
API as Protocol

- **Caller Javascript**
- **App Provider Web Server**
- **Callee Javascript**

- **Caller Browser**
- **Callee Browser**

**Connections:**
- **JS API**
- **Media + Media Path Signaling (ICE/STUN/TURN)**

**Domains:**
- **App Trust Domain**
- **Browser Trust Domain**
API Scope

Caller Javascript

JS API

Caller Browser

P2P Connection Management
FW/NAT Traversal Control
Codec capabilities and selection
Media control
Codec control
Media security
Data Transfer

Media + Media Path
Signaling (ICE/STUN/TURN)
Security Problem 1: DDoS

1. Caller Javascript
2. App Provider Web Server
3. Malicious Website
4. Caller Browser
5. App Trust Domain
6. Browser Trust Domain
7. Media + Media Path Signaling (ICE/STUN/TURN)
8. DDoS Target
Security Problem 2: Protocol Emulation

- Caller Javascript
- App Provider Web Server
- Malicious Website
- App Trust Domain
- Browser Trust Domain
- JS API
- Corporate DNS Server
- Browser packets emulating DNS

Diagram shows the flow from Caller Javascript to App Provider Web Server, passing through a DNS server, with connections labeled for JS API, Browser packets emulating DNS.
Provider Interop Case

Application Provider 1

JS/HTML App

Browser

SIP

Application Provider 1

JS/HTML App

Browser

Media + Media Path Signaling (ICE/STUN/TURN)
Existing Gear Case 1

Application Provider 1

JS/HTML App

Browser

SIP

IP PBX

SIP, MGCP, H323, Proprietary

Media + Media Path Signaling (ICE/STUN/TURN)

JS API
Existing Gear Case 2

Application Provider 1

IP PBX

SIP

Media Gateway

JS/HTML App

Browser

Media + Media Path Signaling (ICE/STUN/TURN)

SIP, MGCP, H323, Proprietary