

Should we support SDES in WebRTC?

draft-ohlsson-rtcweb-sdes-support-00
author: Oscar Ohlsson

Presenter: Hadriel Kaplan



The Question

- We *are* going to mandate DTLS-SRTP be implemented, and *used* much of the time
 - Whenever the far-end does DTLS-SRTP
 - Whenever the Web connection is not HTTPS
- So the question is: should we *also* support SDES?



Photo: Rebecca (Becky/Bex)

Why bother?

1. Reduced complexity for interworking gateways (i.e., less cost/perf-overhead)
2. Allows end-end SRTP for interworking cases
3. Reduced time-to-media
4. It is known to work and be interoperable
5. It's trivial additional complexity, assuming it does not truly degrade security
 - And that's the really big question

The concerns with including SDES

1. Enables eavesdropping
 - Enables malicious websites to snoop
2. No perfect-forward-secrecy
 - Logged SDES keys let one decrypt after-the-fact
3. Susceptible to downgrade attacks
 - Malicious website could force SDES every time
4. Unverifiable
 - Don't know if the media is secure end-end or not
5. Not complicated enough
 - Developers aren't challenged enough



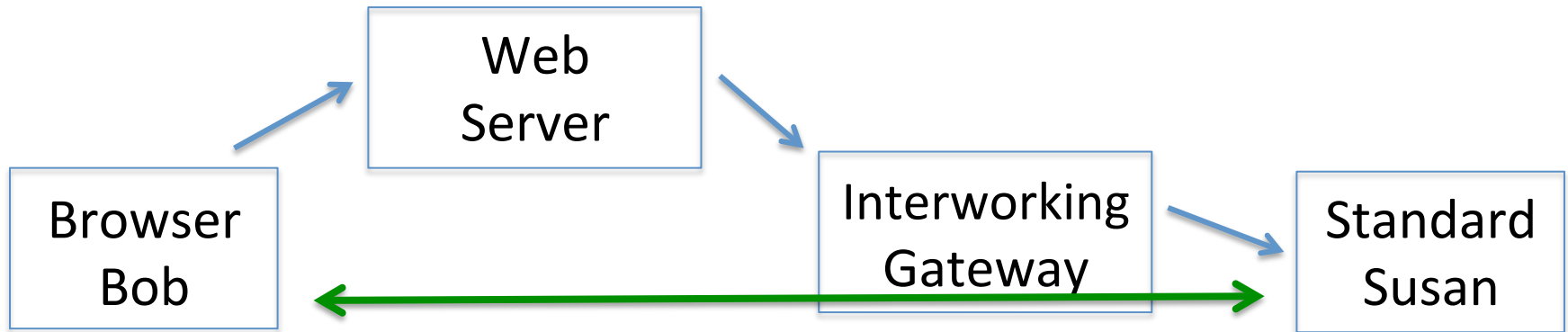
ACME Feedback
Plugin For Wordpress

Get Visitor Feedback
Survey Customers
Pops On Exit Or Click
Increase Time On Site
Popup Videos or Ads
Popup Widgets
And More!

[MORE INFO](#) 

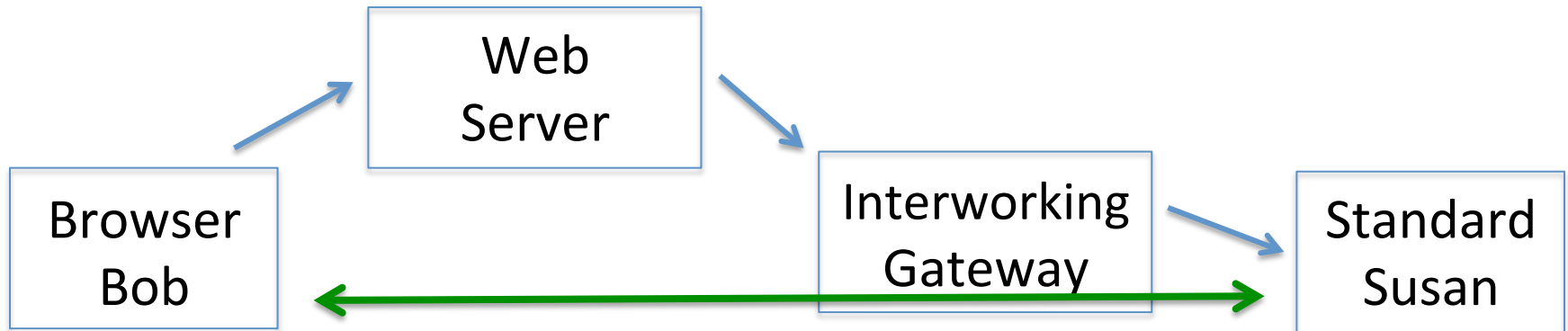
The advertisement features a blue header with the product name and a red-bordered box containing a 3D rendering of the software box. The box is blue and white with the product name and a screenshot of the plugin's interface. To the right of the box, there is a list of features and a 'MORE INFO' button with a yellow arrow pointing right.

Enables Eavesdropping



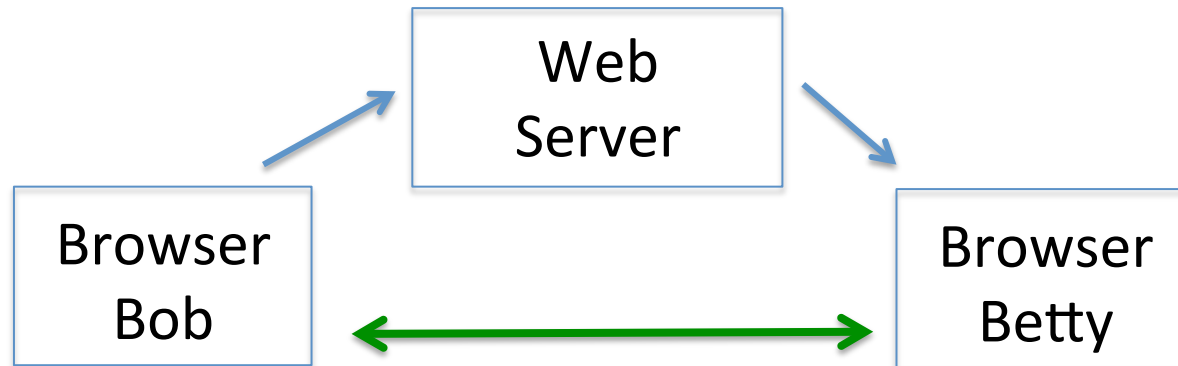
- With SDES, Web-server sees the key
 - IWF gateway sees the key even in DTLS-SRTP
- If evil Web-server force media to go through a path it can snoop, then it can decrypt media
- BUT, it can do that with DTLS-SRTP too
 - It just inserts itself as the IWF Gateway

No PFS



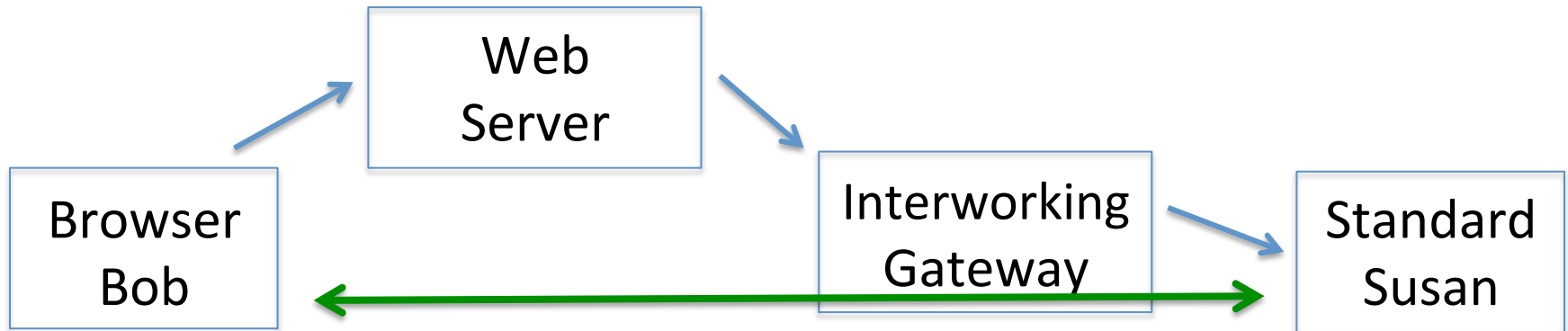
- With SDES, if a session key is ever discovered in the future, past media using it is compromised
 - Of course the media has to actually be available/recorded
- BUT, DTLS-SRTP loses PFS with an IWF gateway too
 - Nothing prevents IWF from logging all keys

Susceptible to downgrade



- Evil Web-Server can make Bob think he's talking through an IWF Gateway, do SDES
- BUT, a Web-Server can already insert itself as a DTLS-SRTP B2BUA
 - It would be cheaper with SDES though

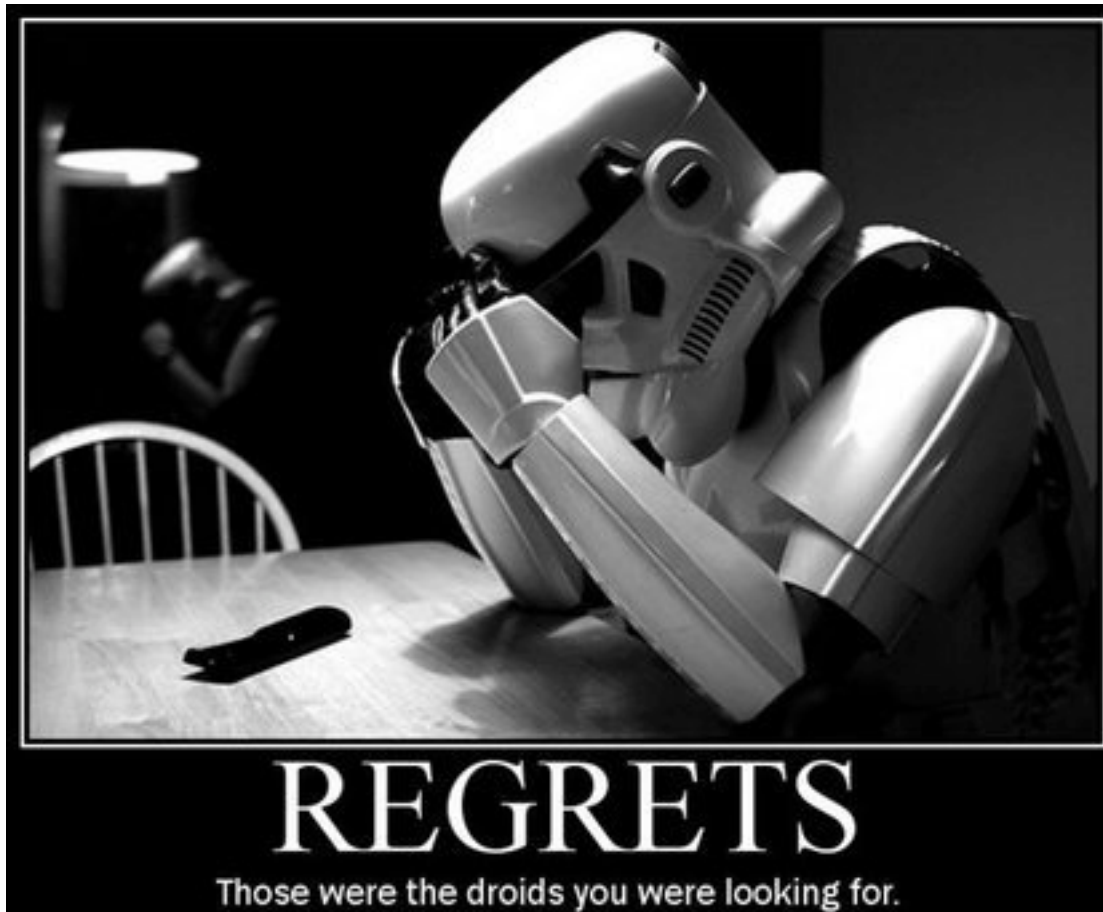
Unverifiable



- With SDES, you don't know if the media is secure end-to-end
- The short answer is “yes you do know: it's NOT secure end-to-end”
 - DTLS-SRTP isn't either, until and unless you verify the keys or we have an IdP solution *deployed*
 - And for interworking cases DTLS-SRTP is not end-to-end secure, but who would know?

What if we're wrong?

- We'd remove/deprecate it
 - Security issues cause updates all the time



We've been told Browsers get upgraded often and quickly

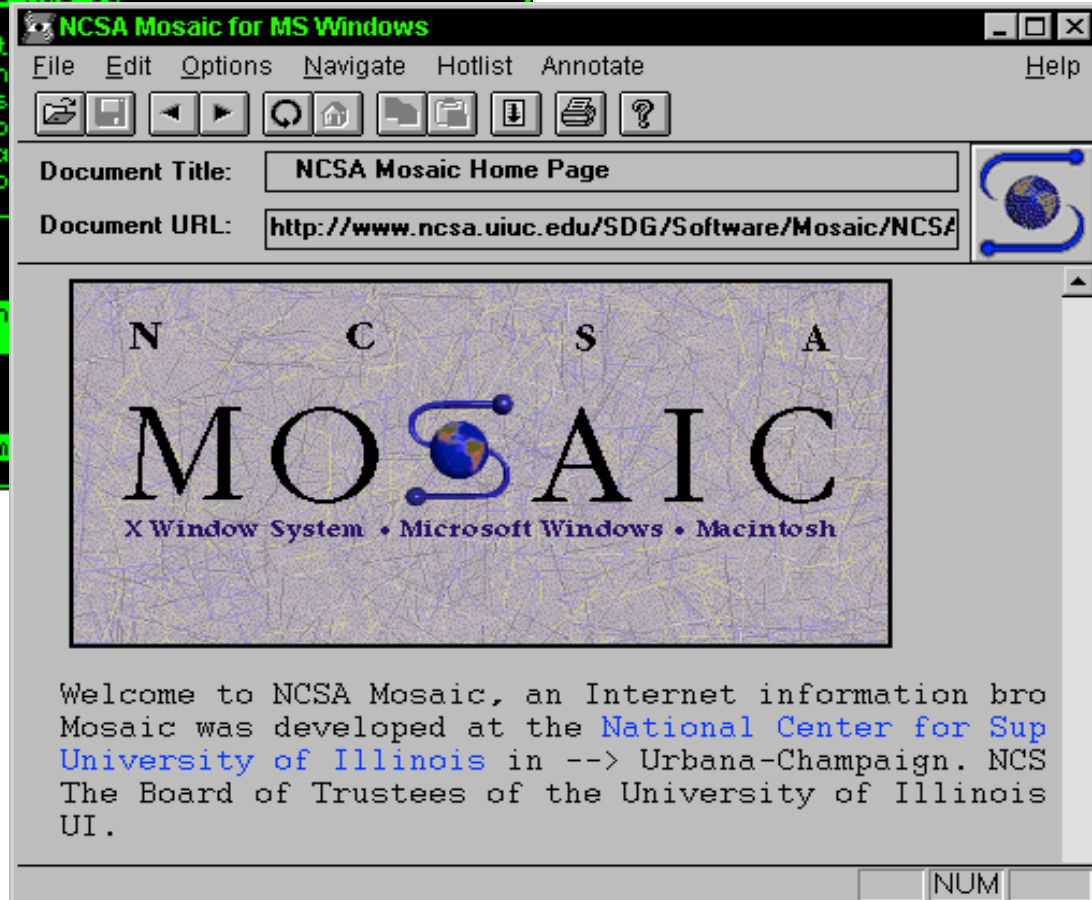
```
(c) GNU General Public License | lynx | 2.8.2 /jh
Q-emuLator (Sinclair QL emulator) support page (p1 of 4)

#home up next! previous

@-emuLator
The QL emulator for Windows and Mac OS

[icon.gif] Q-emuLator is a software-only emulat
an application in the Windows and Mac OS environ
Q-emuLator has an interpreter of the 68008's ins
the basic QL's hardware, redirecting input and o
PC's video, keyboard, mouse, disks, sound hardwa
list of @-emuLator's current features is availab

Index
[windows.gif] - [windows.gif] Q-emuLator for Win
[macos.gif] - [macos.gif] Q-emuLator for Mac OS
Q-emuLator snapshots
Q-emuLator's sources and UQLX
QL technical information
-more- http://users.infoconex.com/dan/le/index.htm
```



Time for the Mic-line

- Let the circus begin...

