The background of the slide features a close-up, low-angle shot of several fiber optic cables. The cables are dark, but their ends are illuminated, creating a series of bright, glowing points of light. These points of light are connected by thin, dark lines, suggesting the paths of the cables. The overall effect is a sense of dynamic energy and connectivity, with the light trails appearing to radiate from the bottom left towards the top right.

Advanced topics in
audio/video conferencing
- Security -

9th SURA/ViDe conference

Atlanta, USA



The why's and the who's and the what's...and whatever else you can think of

- Security in voice/video conferencing is important
 - Many people (often) forget this fact: Yes there are threats on voice and video (and data communication)
- It is not necessarily about “How can I make my H.323 connection work through a firewall?”
- Most of the threats identified by the VoIPSA group for VoIP will apply to videoconference
- Most of the threats are not focused on a particular protocol, though there are many such threats

...a few threats known to man...and women

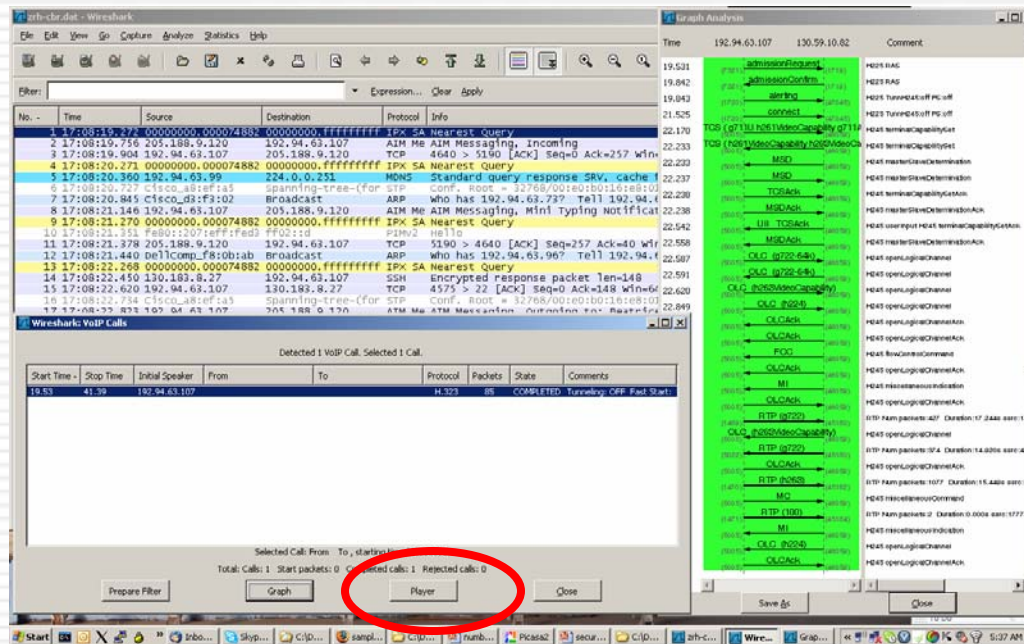
- 6 large areas of threats
 - Social threats
 - Eavesdropping
 - Interception and modification
 - Service abuse
 - Intentional interruption of service
 - Other interruption of service

Some protocol specific threats

- H.323
 - CA-2004-01 Multiple H.323 message vulnerabilities
 - Caused your codec to either restart or freeze
 - Have you ever tried to send flood LRQ/ARQ messages?
- SIP
 - SIP Message flooding
 - Invite/Register flooding
 - Attacker sends a large amount of Invite/Register requests to the 'victim'
 - Invite Response/Register Response flooding
 - Intend to receive authentication information
 - Register Response flooding: Attacker sends Register message with wrong credentials

An eavesdropping sample

- Have you ever made a SIP call between two X-lite clients, and used Ethereal/Wireshark to monitor the traffic?
 - Ethereal/Wireshark can identify VoIP calls (H.323/SIP)
 - Wireshark now even comes with a Player to replay the conversation!



An example for Service abuse

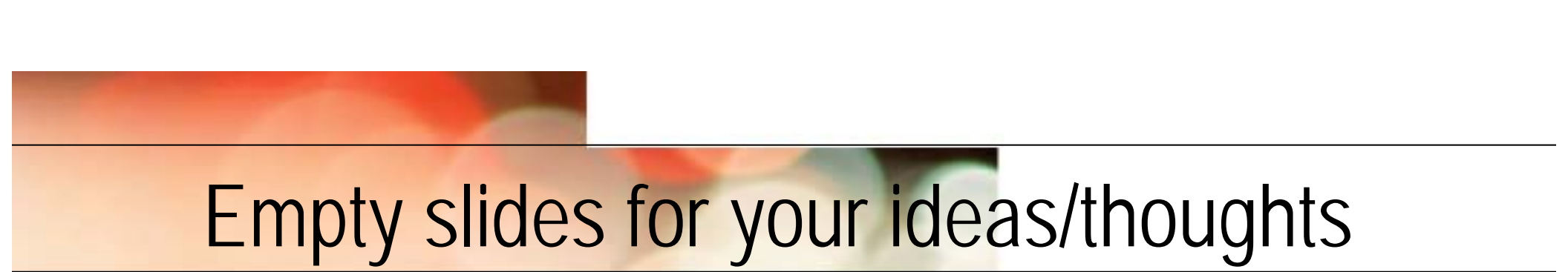
- ISDN calls
 - If you provide ISDN services to staff, make sure to change the dial-out prefix on a regular base
 - Staff/someone else could make very expensive “phone” video calls
 - Proper protection of PSTN/ISDN GW's

A few other things you should pay attention too

- Encryption
 - If you buy new products, make sure that AES/DES is working with your current environment, eg. other endpoints, MCU,...
 - Make sure you also have the license: Some vendors require you to buy an additional encryption pack license, eg. Aethra
- Authentication
 - Authentication in SIP is usually required. This is not the case for H.323 Gatekeeper registrations > Come up with a good scheme, eh. H.350
- Audio/Video mute
 - Make sure your codecs have audio/video mute on auto-answer enabled

References

- Have a look at the “VoIP Security and Privacy Threat Taxonomy” at http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf it is a very good guide with many examples and provides a very good overview
 - More or less all threats on VoIP also apply for Video!!!!



Empty slides for your ideas/thoughts

Thank You

Kewin O. Stoeckigt

kewin.stoeckigt@aarnet.edu.au

+61 3 9211 8446