A Security Analysis of SKYPE

Rodney Thayer

rodney@shmoo.com

Canola & Jones

#include <introduction.h>

- Who's Rodney?
- Why look at Skype?
- Is there a problem?
- Is this talk going to help the bad guys?
- Disclosure policy
- Evaluation strategy

Canola & Jones

End-user Evaluation

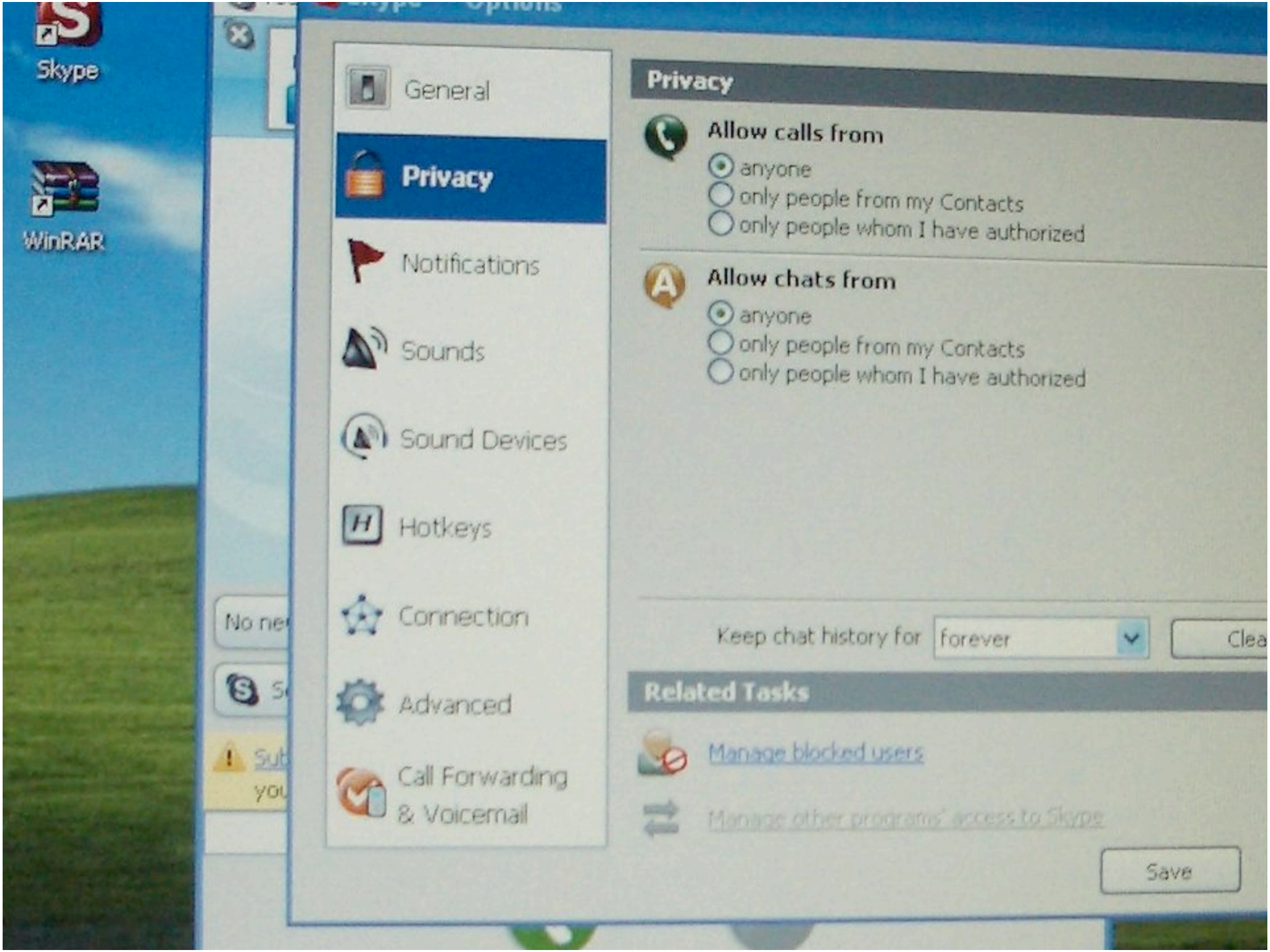
Canola & Jones

OOB Experience

- Download from ‘net – ok
- Standard sort of installer – ok
- Test call capability – nice
- Privacy warnings – poor
- Use of audio – dodgy
- Another chat service -- nice

Provisioning

- Information leakage
- No warnings to end user
- Signal generated when you go on-line


Skype
WinRAR
General
Privacy
Notifications
Sounds
Sound Devices
Hotkeys
Connection
Advanced
Call Forwarding & Voicemail
Privacy
Allow calls from
anyone
only people from my Contacts
only people whom I have authorized
Allow chats from
anyone
only people from my Contacts
only people whom I have authorized
Keep chat history for
forever
Related Tasks
Manage blocked users
Save

Full Name

Gender

Birthdate

dd mm yyyy

Day Month Year

Country/Region United States

State/Province

City

Language English

Home phone

Office phone

Mobile phone

Enter number with country code, for example: +155 55551234

Homepage http://

About Me

Details that only my contacts will see

Change...

Reset to Default

Private details

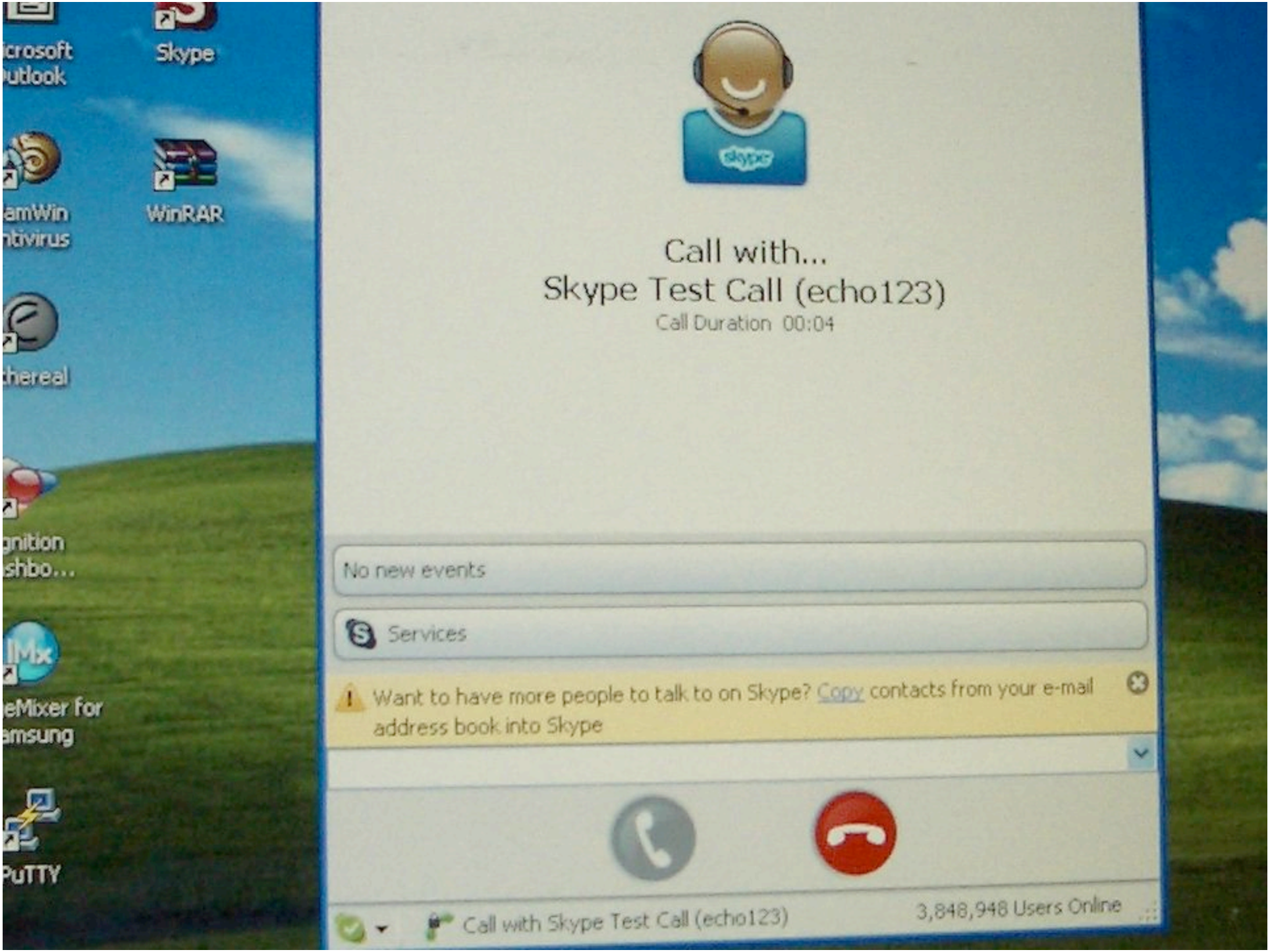
E-mail

Add more e-mail addresses.

Your e-mail will be kept private, but those who know it will be able to use it to search for you on Skype.

Calls

- Audio is dodgy
- Call process is accident-prone
- Sensitive to network (?) load
- Calls sometimes drop
- Call quality vaguely relates to suck-o-meter
- “Hey, it’s free. What’s your problem?”


Skype
WinRAR
Call with...
Skype Test Call (echo123)
Call Duration 00:04
No new events
Services
Want to have more people to talk to on Skype? Copy contacts from your e-mail address book into Skype
Call with Skype Test Call (echo123)
3,848,948 Users Online
PuTTY

Problems

- Calls drop
- Microphone switches on during calling
- Call does not end after voice mail

Conclusions – End User

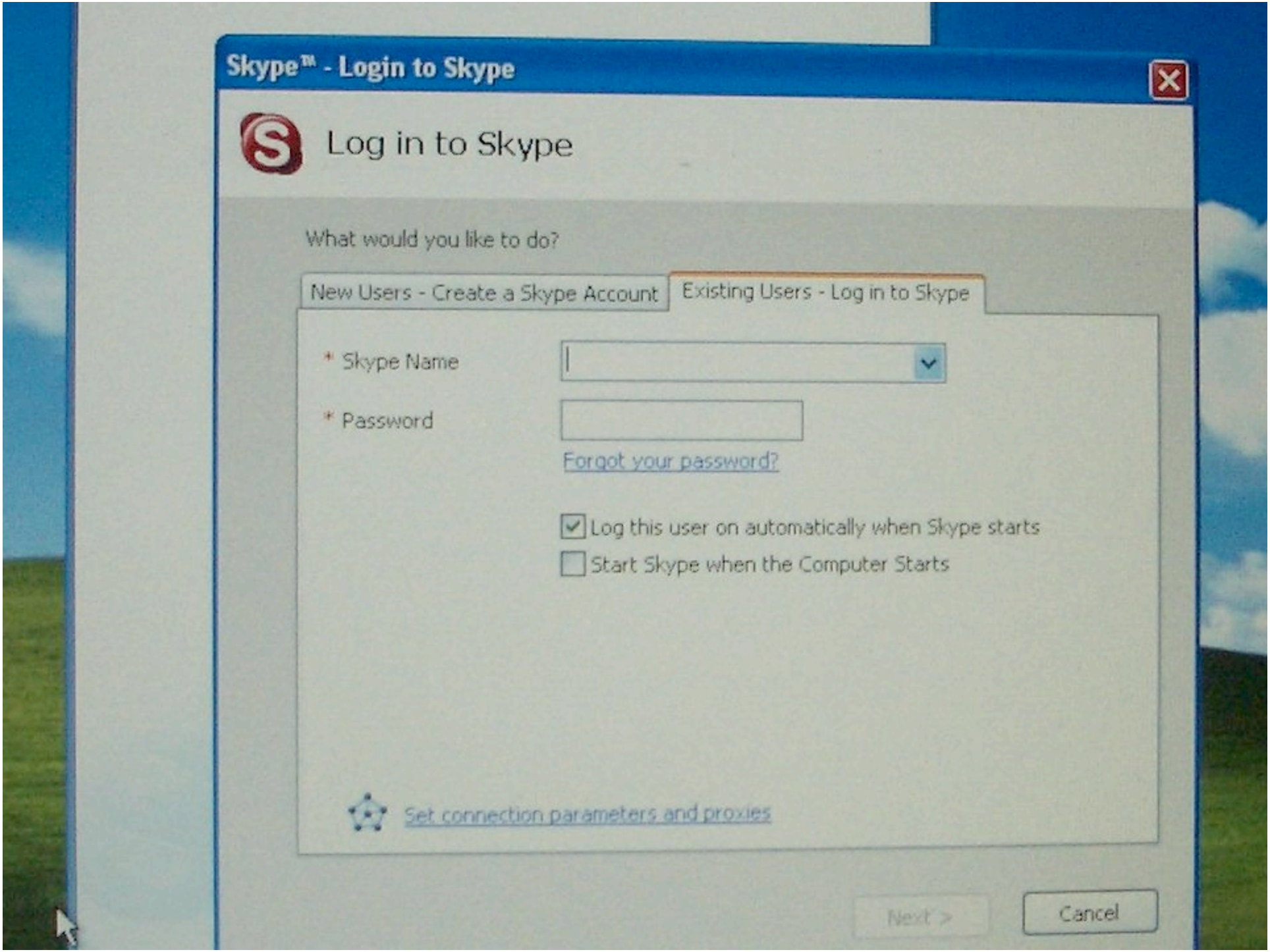
- It leaks information
- It's flakey
- It goes into "audio bug" mode at random
- It's free and so dangerously popular
- Chat is (encrypted?) therefore dangerous IM

Engineering Evaluation

Canola & Jones

Application Construction

- Presumes low-privacy configuration
- Not quite a proper windows application
- Start-up logic leaks information
- Resource theft as network use model


Skype™ - Login to Skype
Log in to Skype
What would you like to do?
New Users - Create a Skype Account
Existing Users - Log in to Skype
* Skype Name
* Password
Forgot your password?
Log this user on automatically when Skype starts
Start Skype when the Computer Starts
Set connection parameters and proxies
Next >
Cancel

Resource Usage

- It’s Kazaa
- You wanted to share didn’t you?
- Have you considered what your IT department might thing of this?

Canola & Jones

Latvia?

Active Connections

Proto	Local Address	Foreign Address	State
TCP	sb2:http	sb2:0	LISTENING
TCP	sb2:epmap	sb2:0	LISTENING
TCP	sb2:https	sb2:0	LISTENING
TCP	sb2:microsoft-ds	sb2:0	LISTENING
TCP	sb2:5679	sb2:0	LISTENING
TCP	sb2:62729	sb2:0	LISTENING
TCP	sb2:1025	sb2:0	LISTENING
TCP	sb2:netbios-ssn	sb2:0	LISTENING
TCP	sb2:1975	wash.svnets.lv:https	ESTABLISHED

During a call

Active Connections

Proto	Local Address	Foreign Address	State
TCP	192.168.253.128:1975	213.182.207.240:443	ESTABLISHED
TCP	192.168.253.128:2071	67.162.96.210:32040	SYN_SENT
TCP	192.168.253.128:2072	24.8.222.148:2073	SYN_SENT
TCP	192.168.253.128:2073	202.156.72.119:64488	SYN_SENT
TCP	192.168.253.128:2074	67.184.166.203:13640	SYN_SENT
TCP	192.168.253.128:2075	83.253.110.133:38104	SYN_SENT
TCP	192.168.253.128:2076	67.175.218.8:16754	SYN_SENT

Canola & Jones

Conclusions – Engineering

- It leaks privacy unless uncomfortably controlled
- It's a file sharing app
- It's a poster child for policy enforcement
- Oh, by the way, it's a non-standard protocol and therefore by definition insecure

Shiny! Let's be bad guys.

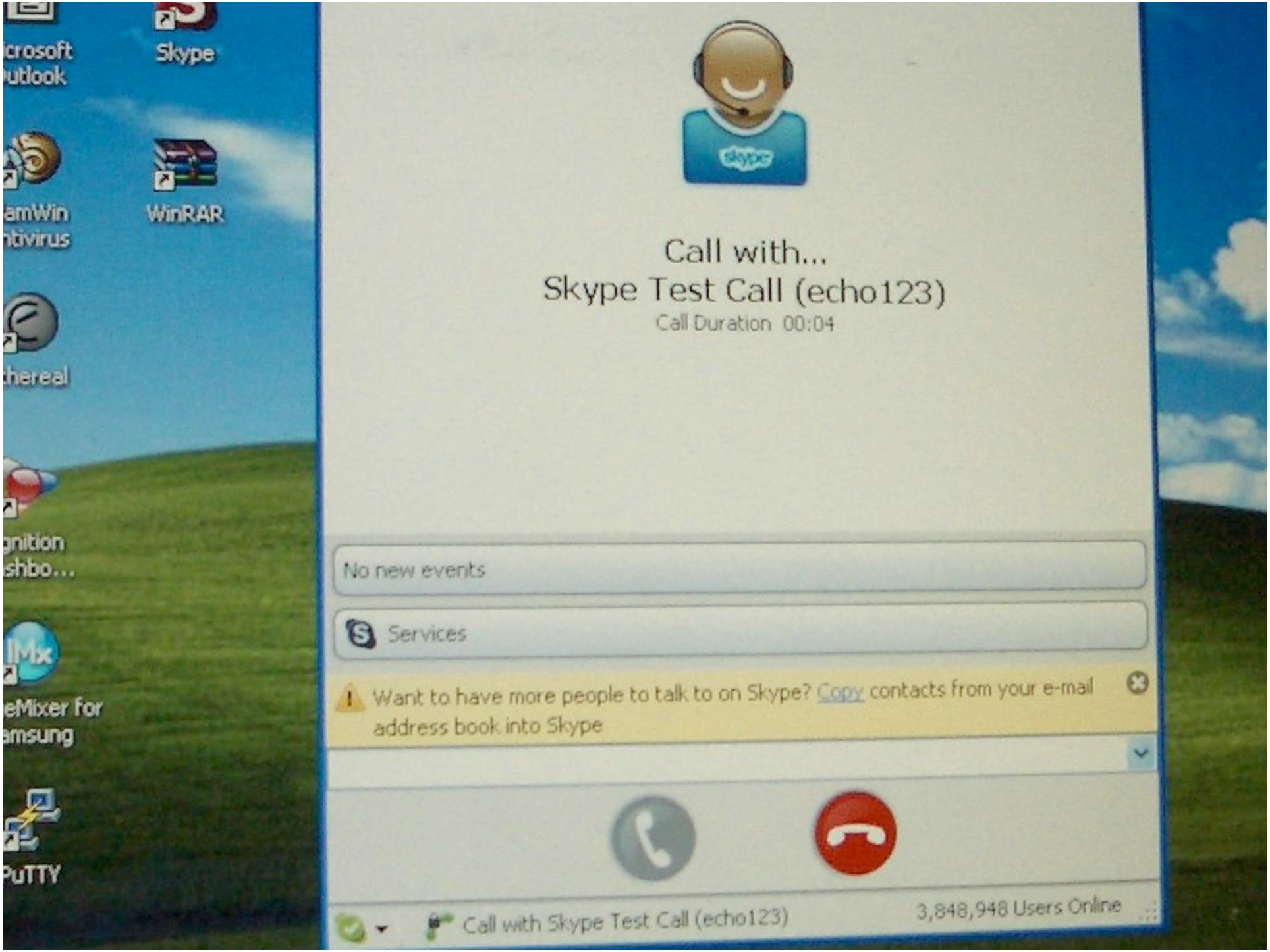
Jayne (Serenity)

Recon – Application

- The windows application itself (bug, normal sploits)
- Media drivers it uses
- Configuration information

Recon - Infrastructure

Canola & Jones


Skype
WinRAR
Call with...
Skype Test Call (echo123)
Call Duration 00:04
No new events
Services
Want to have more people to talk to on Skype? Copy contacts from your e-mail address book into Skype
Call with Skype Test Call (echo123)
3,848,948 Users Online
PuTTY

Full Name

Gender

Birthdate

dd mm yyyy

Day Month Year

Country/Region United States

State/Province

City

Language English

Home phone

Office phone

Mobile phone

Enter number with country code, for example: +155 55551234

Homepage http://

About Me

Details that only my contacts will see

Change...

Reset to Default

Private details

E-mail

Add more e-mail addresses.

Your e-mail will be kept private, but those who know it will be able to use it to search for you on Skype.

Recon – Infrastructure

- Well marked alternative targets
- Protocol exploits
- Protocol hijack
- Directory

Exploit-enabling features

- Phone phishing
- Stalking
- Identity theft
- Network resource stealing
- Social engineering attacks

Possible exploits

- Turn on the mic and make the pc a bug
- Call/chat to exploit the victim skype application
- Protocol hacks
- Protocol dos attacks
- Bypass firewall/ids/ips via net sharing
- Grafitti via chat

Update

- E-Bay purchases Skype
- Skype vulnerabilities we're chasing
- Lessons from looking at Skype

Conclusions

Canola & Jones

Conclusions

- Soft phones are a new class of exploit target
- Multimedia is still hard
- Skype has risks
- Soft phones have risks – not more than instruments but not nothing
- Try a real VoIP service using standards-based protocols
- Watch out for phone attacks

Slides will be at

http://www.canola-jones.com/presentations

rodney@canola-jones.com

Canola & Jones