WWW Presentation- April 24, 2008

Privacy-Enhanced Sharing of Personal Content on the Web

Mohammad Mannan and P. C. van Oorschot

Carleton University, Canada

The need for sharing is real

People want to share:

- photos, contact info
- "What are you doing?"
- preferences, opinions

Sharing is easy

Popular techniques:

- Social networking sites, blogs
- Cheap (or free) personal web space

But maintaining "privacy" is not so easy.

Common solutions for privacy

Popular techniques:

- Passwords (distribution, retraction)
- Obscure web links
- “Friends’ circle” on social networking sites

Privacy in social networking sites – Usability

1. Build the friends' circle (without annoying others?)

2. Viewers must join the same network as the publisher

3. Publisher is restricted to a particular site

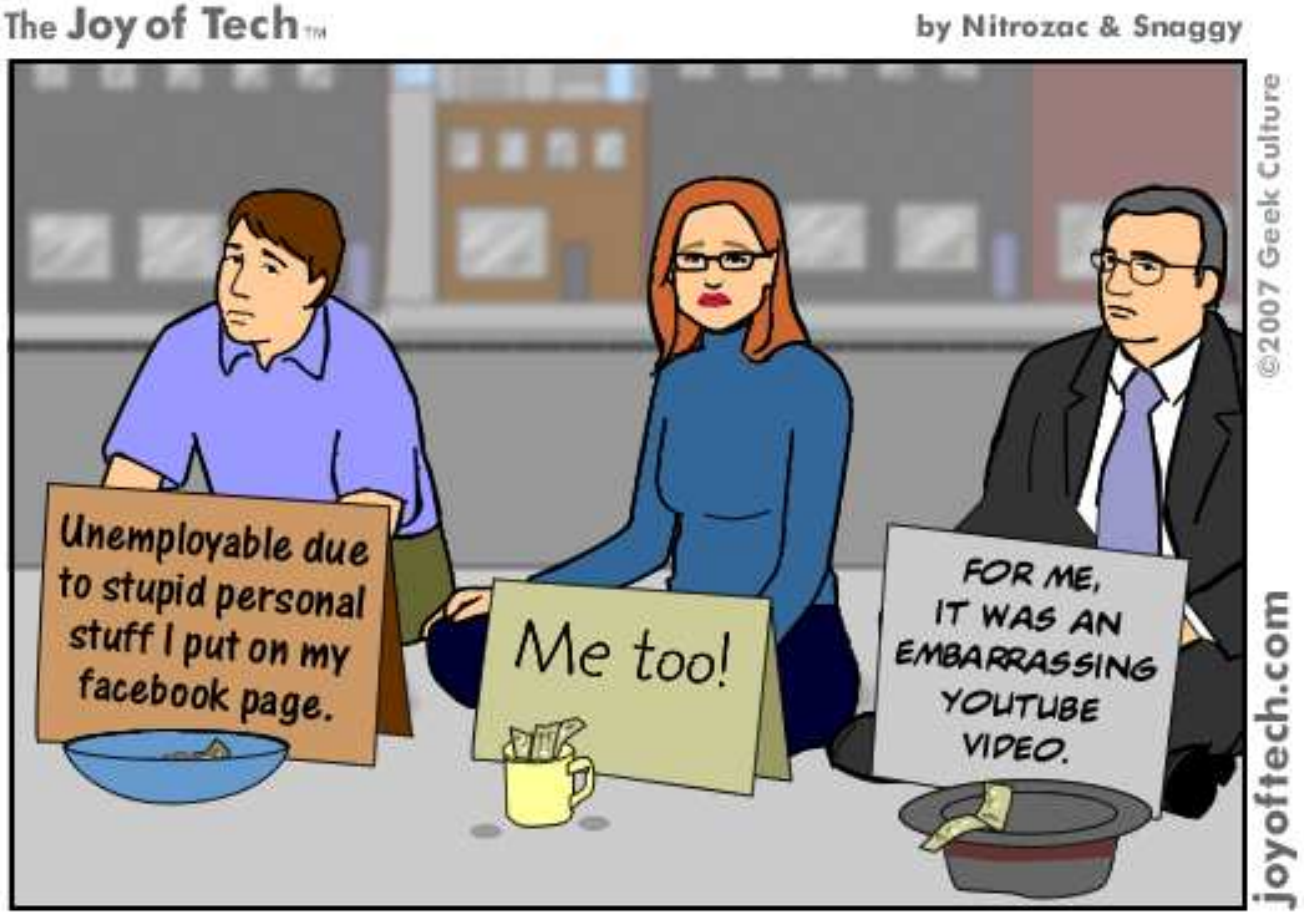
So your profile is “privacy-protected”

– but you forgot about the “U.S. Patriot Act”

– also forgot to read the site’s privacy policy

(Facebook “beacon”, no deleting of accounts)

Consequences: job lost



Signs of the social networking times.

Consequences: job denied

You have “cleaned” your profile before an interview

– but profiles are incrementally archived

Consequences: targeted phishing/malware

Secret Crush virus spreading on Facebook

Malicious widget promises to reveal who fancies you

James Rivington

04 Jan 2008 12:36 GMT

A spyware-infested third-party widget on Facebook is spreading like wildfire. Like some kind of e-STI, the 'Crush' application is spreading malicious spyware to young hopefuls who're looking to find love online.

Don't let your heart be crushed by the latest Facebook exploit

zoom

Problem statement

1. How to share personal content on the web among selected peers
2. Goals:
   - share only within a “circle of trust”
   - deny access to strangers, web crawlers, auto-indexers
   - usable security

Military-grade security is a non-goal

Our proposal: overview

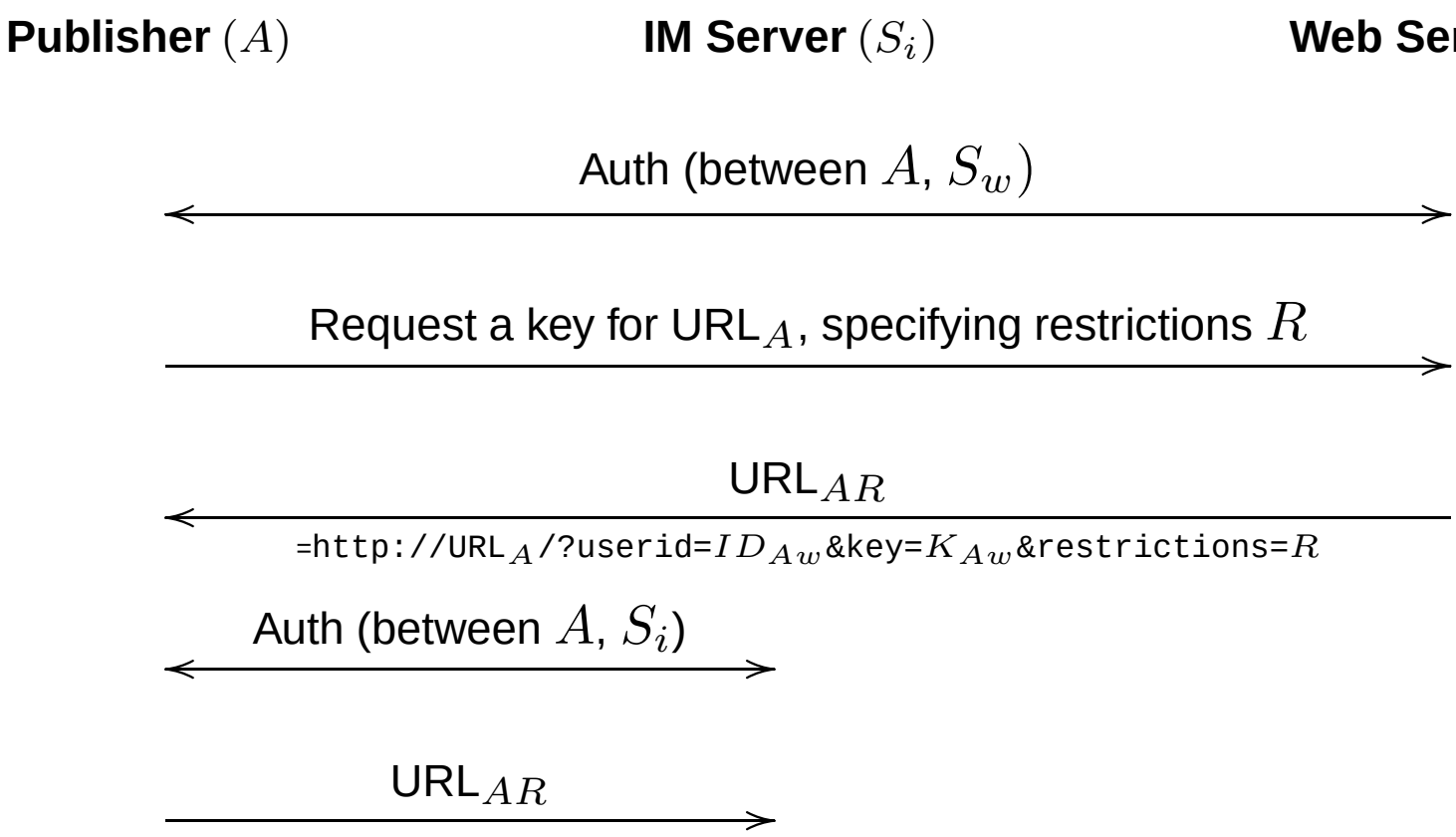
IMPECS: IM-based Privacy-Enhanced Content Sharing

- only a publisher's IM contacts can view her web page
- IM and web servers share a user-specific key
- IM server generates a 'ticket' for a viewing user (contact)
- Web server validates the ticket before serving content

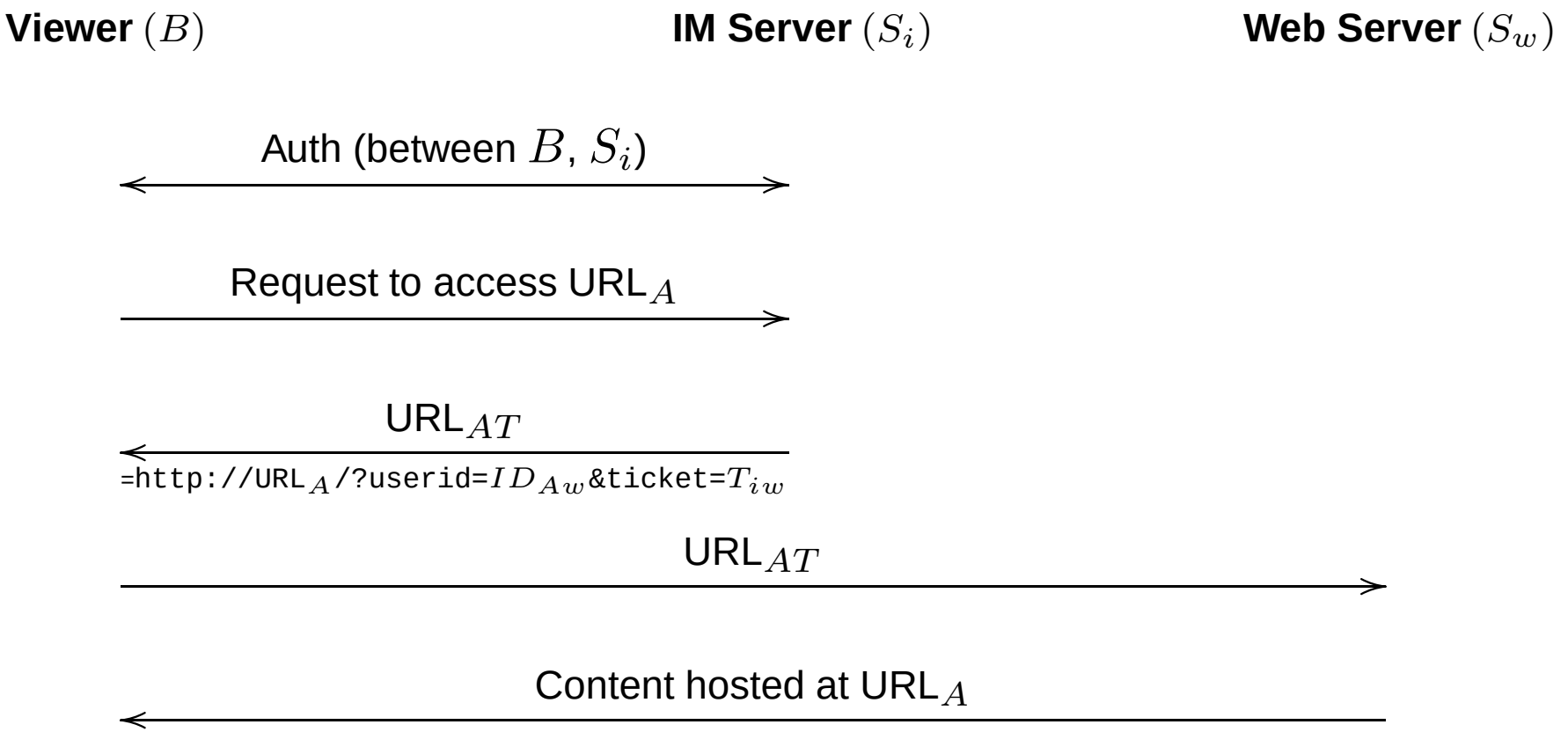
Notation used in IMPECS

A, B	Two IM users Alice and Bob
S_i, S_w	IM and web servers
ID_{Aw}	A's user ID at S_w which is unique in S_w's domain
K_{Aw}	A's content sharing key, shared with both S_w and S_i
URL$_A$	The URL of A's publishing web folder on S_w
R	A set of access restrictions on URL$_A$ as imposed by A
T_{iw}	$= \{ID_{Aw}, R\}_{K_{Aw}}$ (access control ticket for viewing URL$_A$)

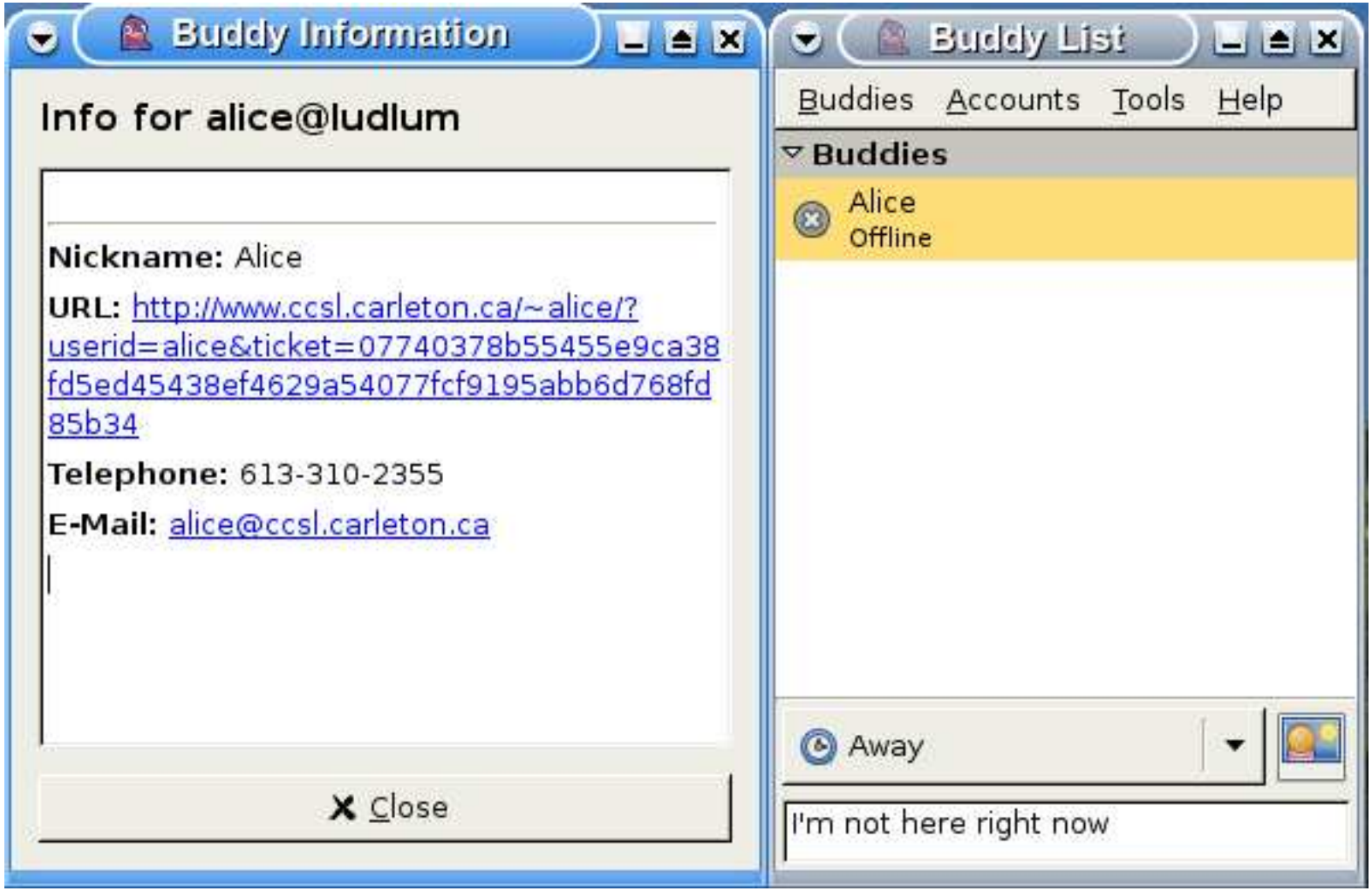
Registering a URL in IMPECS



Viewing a personal URL in IMPECS



IMPECS in action



IMPECS – Advantages

1. Privacy-friendly sharing
2. ‘Improved’ usability
3. Interoperability – publish ‘anywhere’
4. Decreased risks related to sharing

IMPECS – Shortcomings

1. Must use IM
   - – modification of IM server source code
   - – may require IM client updates
   - – needs to run PHP scripts at the web server
2. Malicious contacts may copy and publish personal content on public forums
3. Only as secure as the underlying IM and web protocols

Concluding thoughts

1. Any pre-arranged grouping can be used as “circle of trust”
2. How to protect against compromised/malicious IM and web servers?
3. How to make people privacy-aware?

Thank you ☺

Question/Comments?

mmannan@scs.carleton.ca

http://www.ccsl.carleton.ca