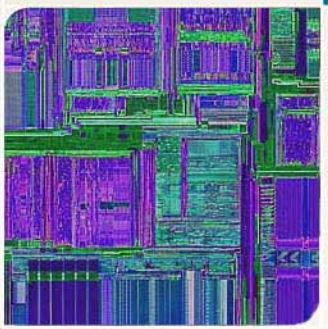
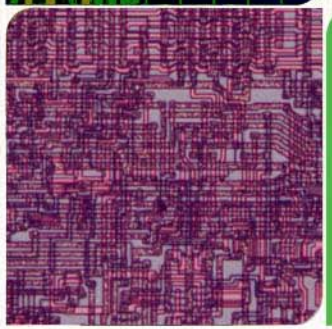
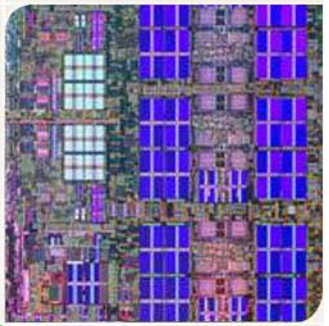
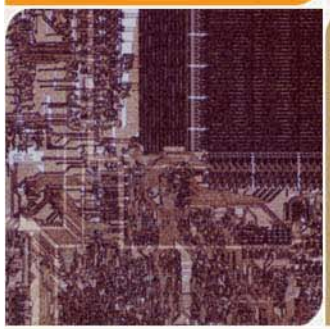






xBook: Redesigning Privacy Control in Social Networking Platforms

Kapil Singh, Sumeer Bhola and Wenke Lee

Georgia Tech College of Computing

Social networking is growing…



facebook

twitter

orkut beta

myspace .com

hi5

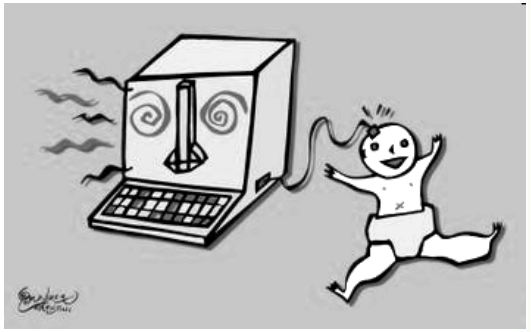
bebo

LinkedIn

xanga

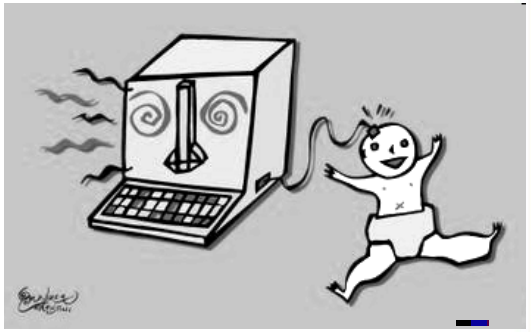
Privacy concerns are growing…

- More personal data being fed to social networks



Privacy concerns are growing…

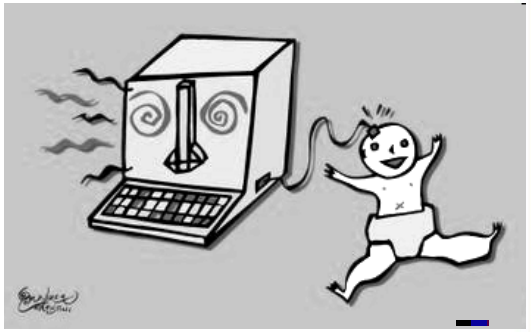
- More personal data being fed to social networks



Op-Ed: Post a photo, wear a pirate hat on myspace, and say goodbye to your career

Privacy concerns are growing…

- More personal data being fed to social networks

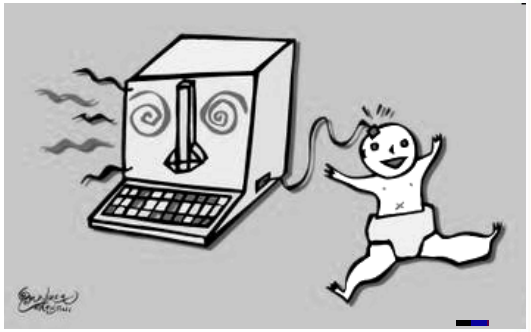


Op-Ed: Post a photo, wear a pirate hat on myspace, and say goodbye to your career

Mayor in MySpace photo flap asked to resign

Privacy concerns are growing…

- More personal data being fed to social networks



Op-Ed: Post a photo, wear a pirate hat on myspace, and say goodbye to your career

Mayor in MySpace photo flap asked to resign

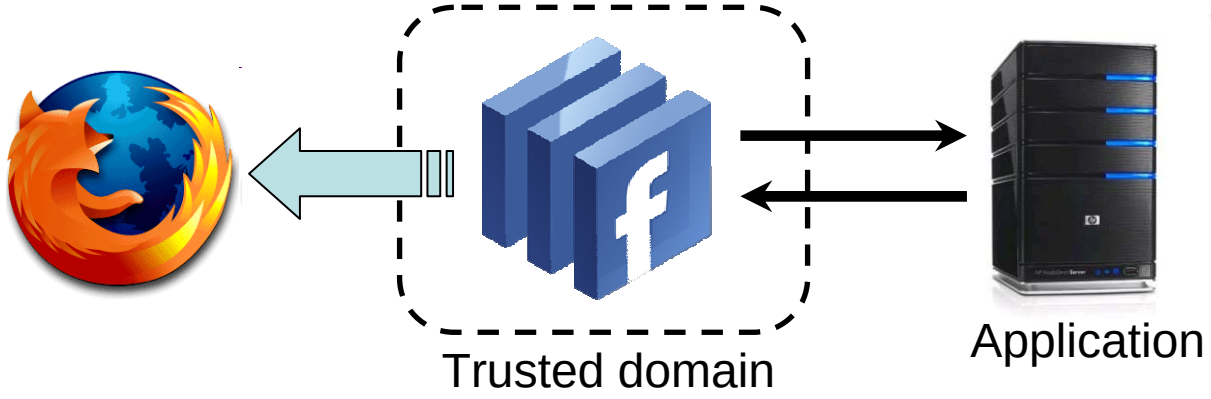
Hoover Police officers arrest Facebook burglary suspects



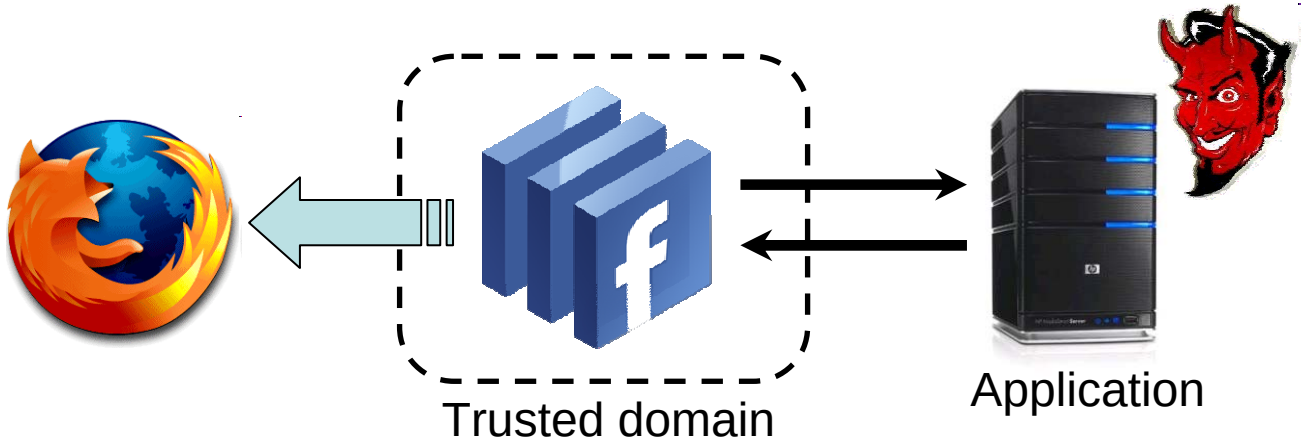
Social Networks as Platforms

- Social networks now act as programming platforms: third party applications.
- Integration with the platform
  - Set of APIs allow an application to have access to user content and integrate into user's profile

Social Platform Architecture

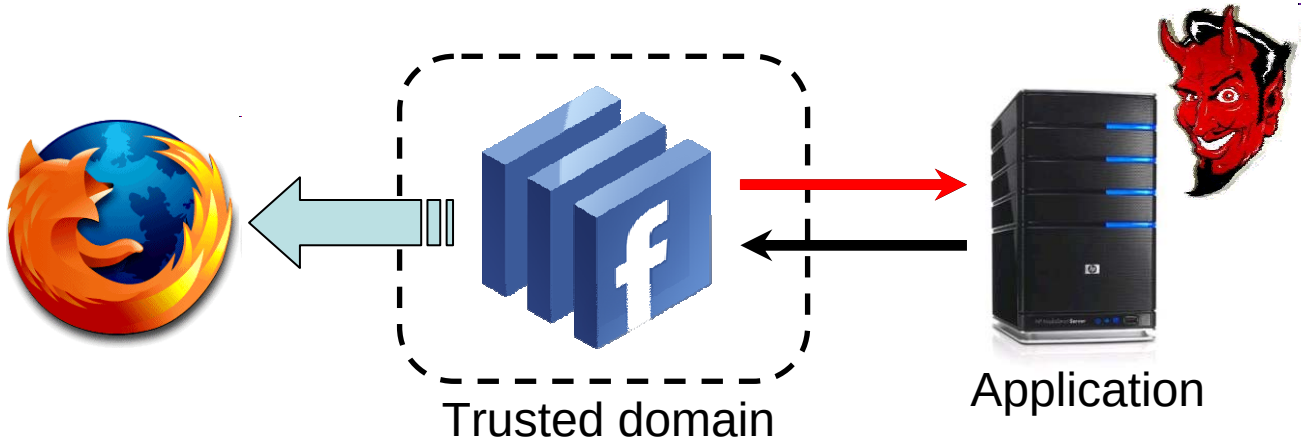


Social Platform Architecture



No control over who can develop and deploy an application.

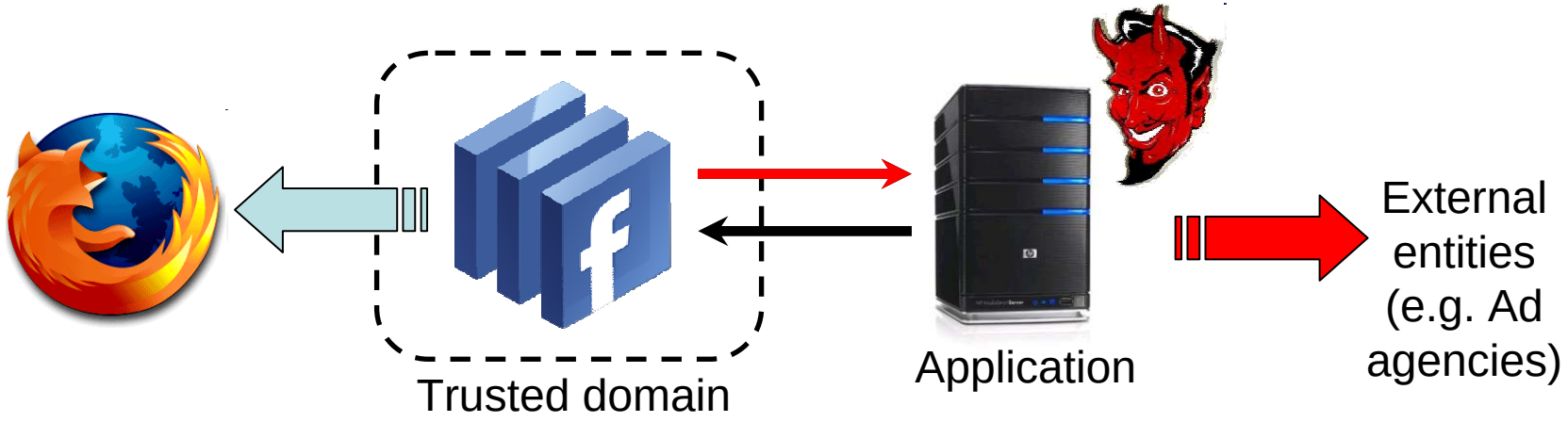
Social Platform Architecture



No control over who can develop and deploy an application.

Minimal or no control on what these applications can access.

Social Platform Architecture

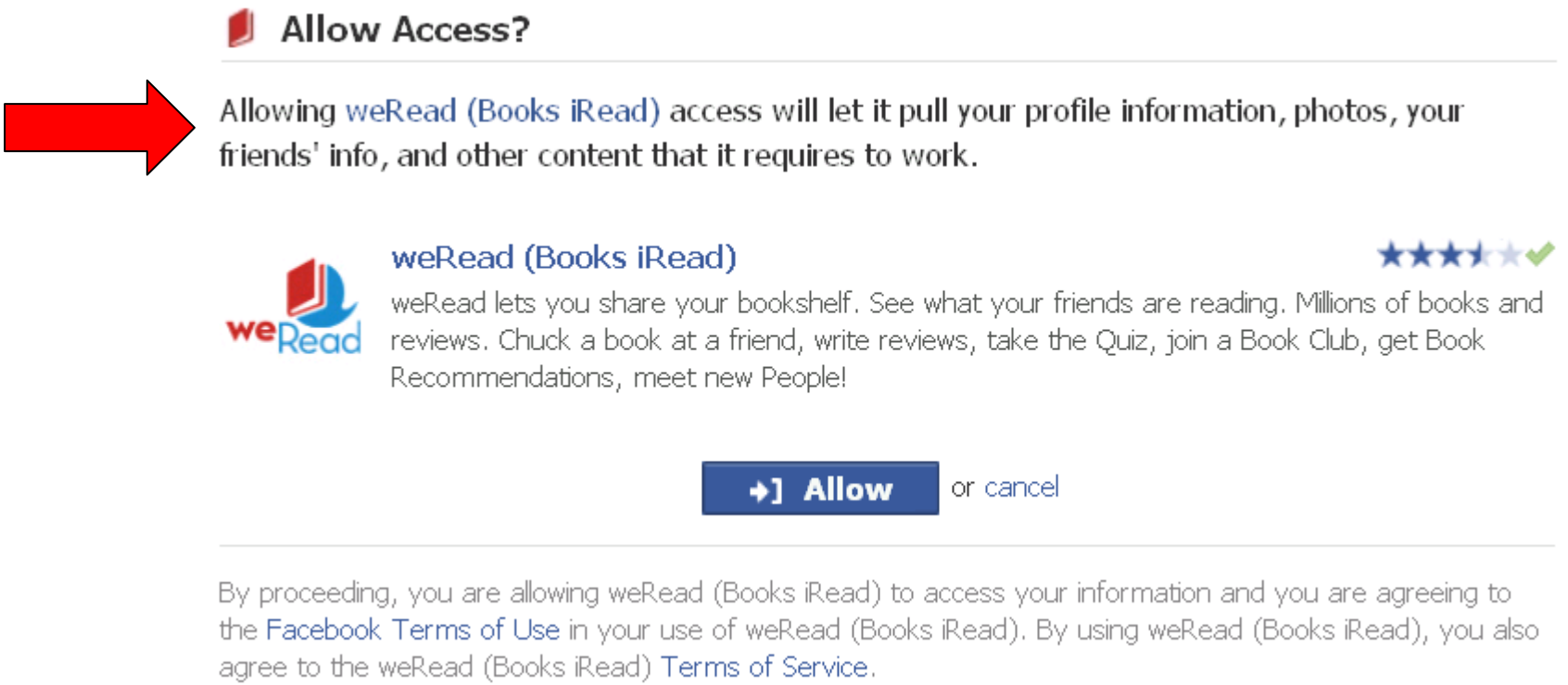


No control over who can develop and deploy an application.

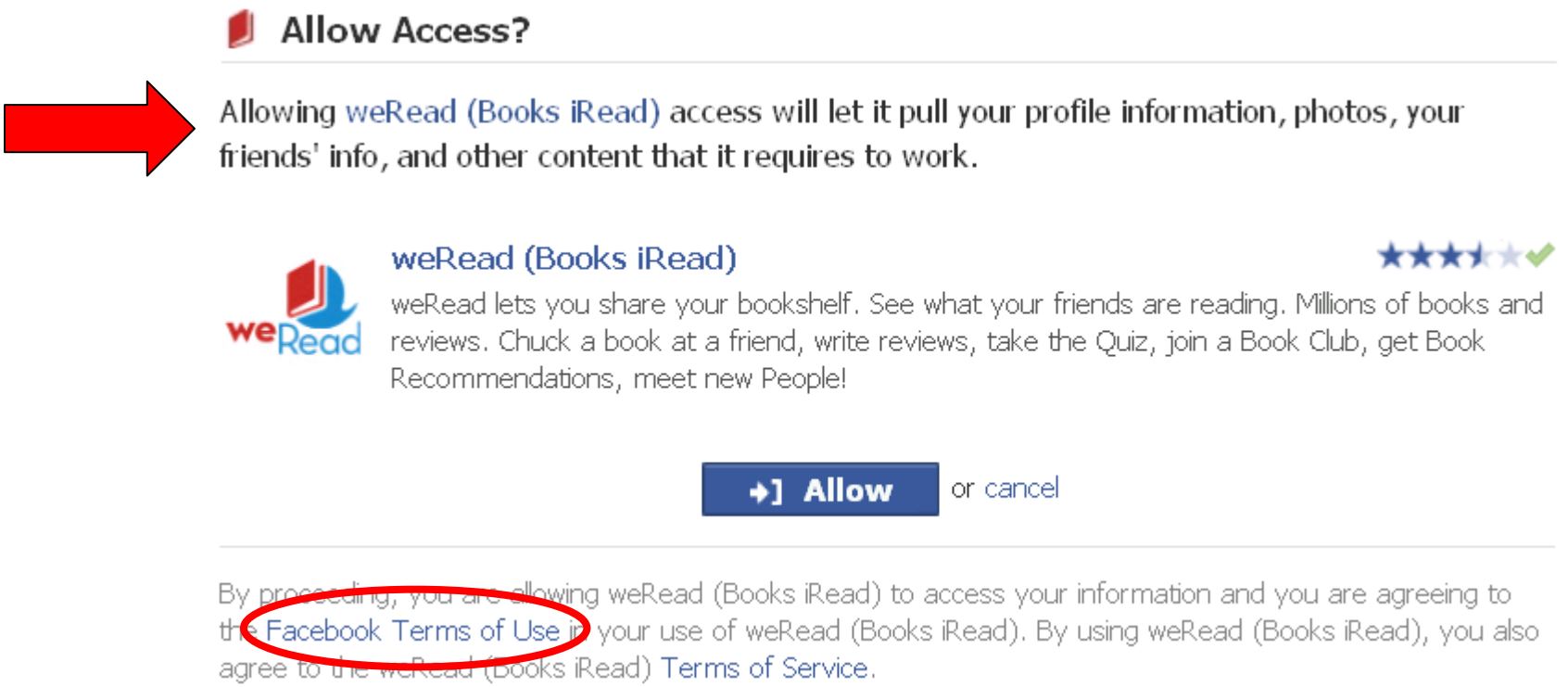
Minimal or no control on what these applications can access.

No control on what an application can do with what it can access.

Current Affairs: Facebook



Current Affairs: Facebook





Facebook's privacy policy is insufficient…

If you, your friends, or members of your network use any third-party applications developed using the Facebook Platform ("Platform Applications"), those **Platform Applications may access and share certain information about you with others** in accordance with your privacy settings. You may opt-out of any sharing of certain or all information through Platform Applications on the Privacy Settings page. In addition, third party developers who have created and operate Platform Applications ("Platform Developers"), **may also have access to your personal information (excluding your contact information) if you permit Platform Applications to access your data.** Before allowing any Platform Developer to make any Platform Application available to you, Facebook requires the Platform Developer to enter into an agreement which, among other things, requires them to respect your privacy settings and strictly limits their collection, use, and storage of your information. However, while we have undertaken contractual and technical steps to restrict possible misuse of such information by such Platform Developers, **we of course cannot and do not guarantee that all Platform Developers will abide by such agreements. Please note that Facebook does not screen or approve Platform Developers and cannot control how such Platform Developers use any personal information that they may obtain in connection with Platform Applications.**



Facebook applications

- Users need to trust the applications.
- Mistakes are made:
  - "Top Friends" application allowed access to the profile of anyone using the application.
  - "We *expect* third-party apps to follow the rules the users set" – director at Facebook.
- Deliberate "mistakes" are made:
  - "Google confirms Adsense ads, security problems in Facebook applications"



Facebook applications

- Users need to trust the applications.
- Mistakes are made:
  - "Top Friends" application allowed access to the profile of anyone using the application.
  - "We *expect* third-party apps to follow the rules the users set" – director at Facebook.
- Deliberate "mistakes" are made:
  - "Google confirms Adsense ads, security problems in Facebook applications"

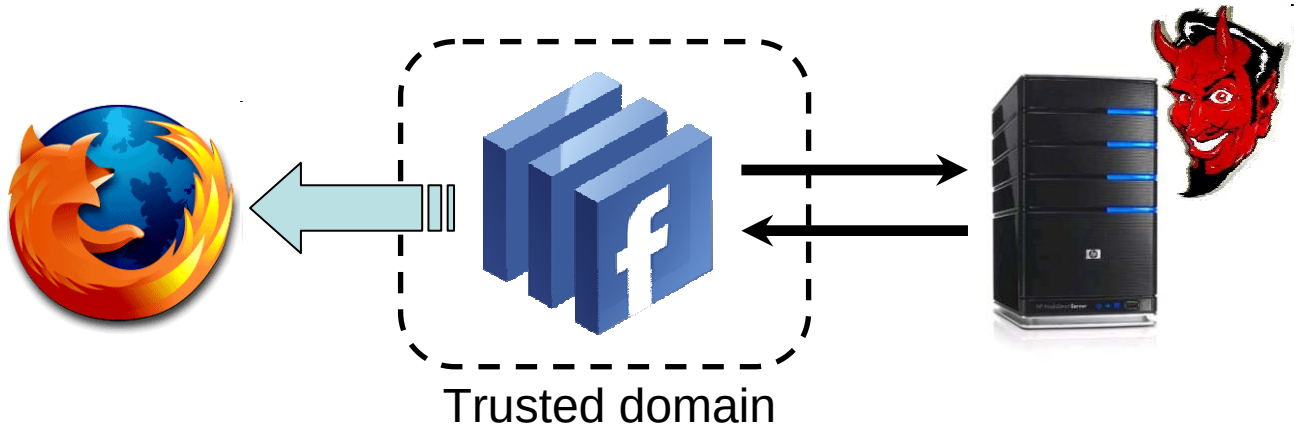
No enforcement, because it is not possible in the current architecture!



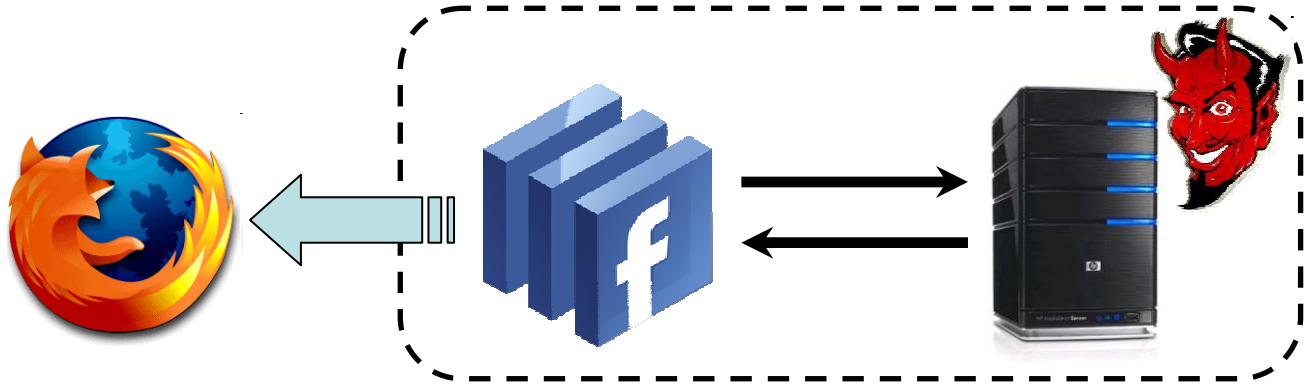
Our Goals

- Provide privacy protection for users' data in presence of third party applications.
  - Prevent data leaks out to external entities.
  - Provide user-user access control (for data flowing through an application).
  - Protection of application's proprietary data.
- No changes should be required on the browser side.
- The user should be oblivious to any design changes.

Our Solution: xBook

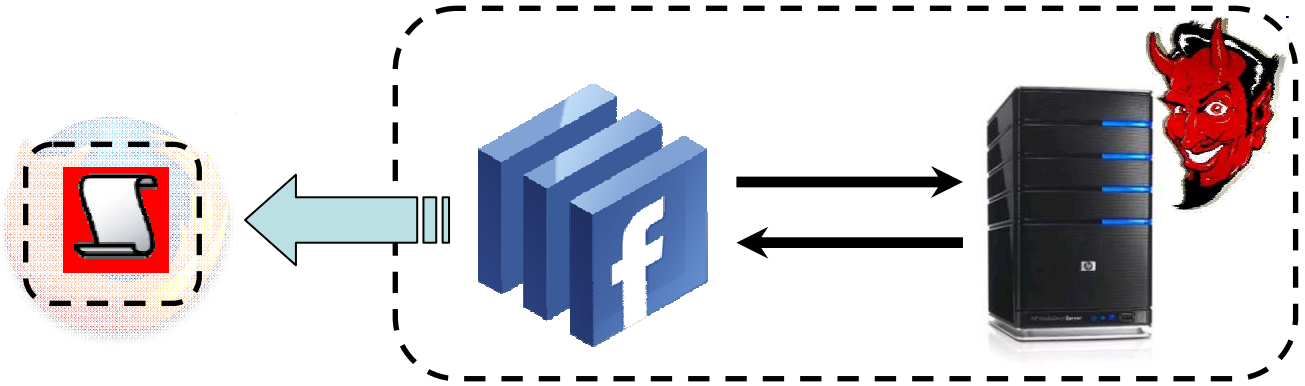


Our Solution: xBook



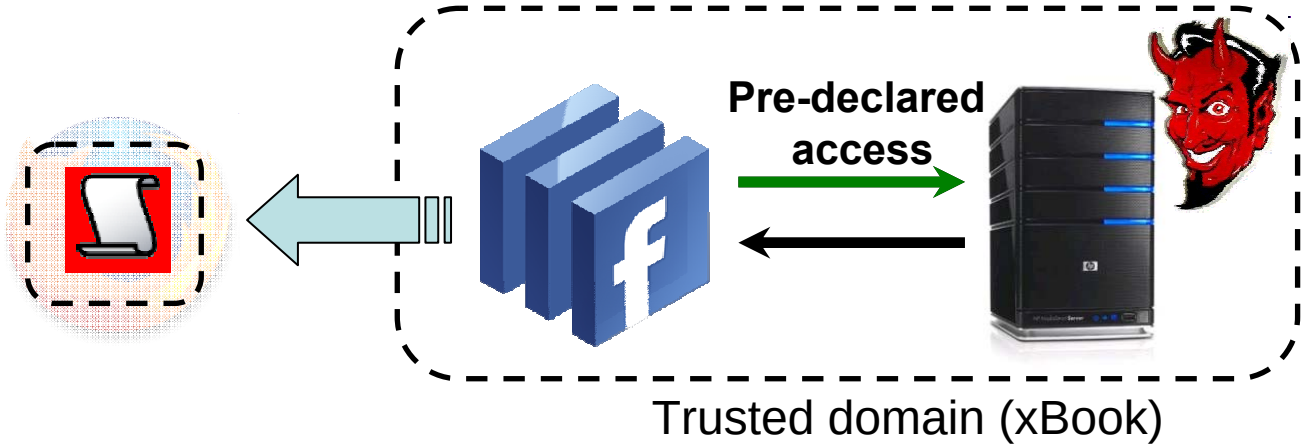
- Pull the applications into the trusted xBook domain.

Our Solution: xBook



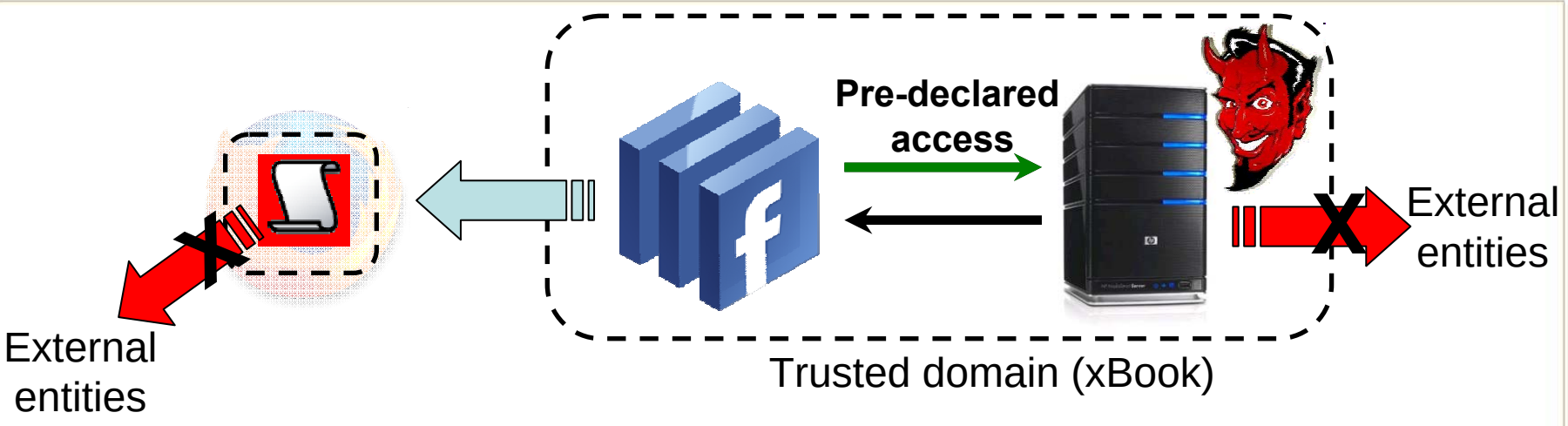
- Pull the applications into the trusted xBook domain.
- Monitor the applications at runtime in the browser.

Our Solution: xBook



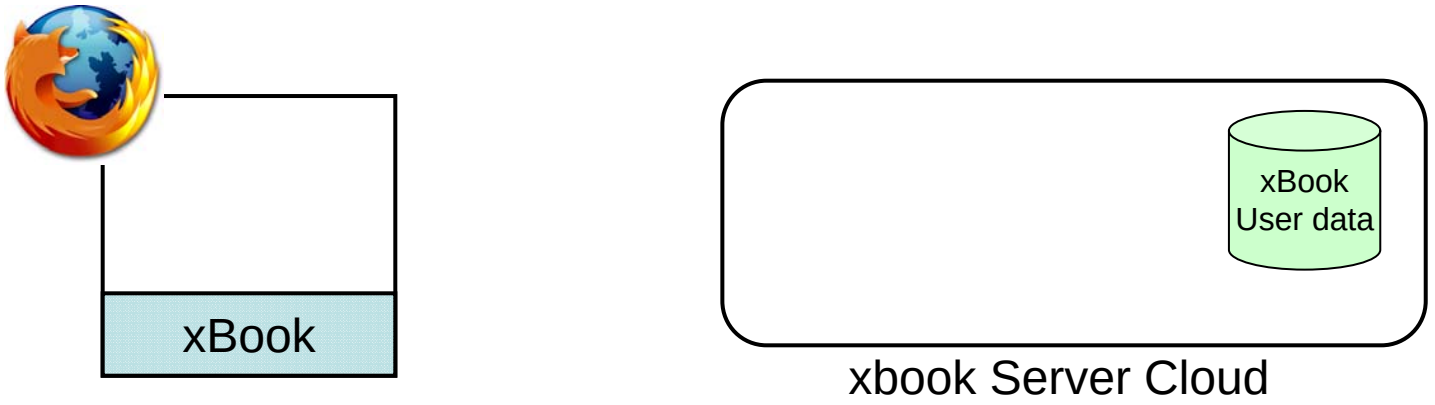
- Pull the applications into the trusted xBook domain.
- Monitor the applications at runtime in the browser.
- Allow applications access to any user data, but *require* them to make use of that data explicit.

Our Solution: xBook



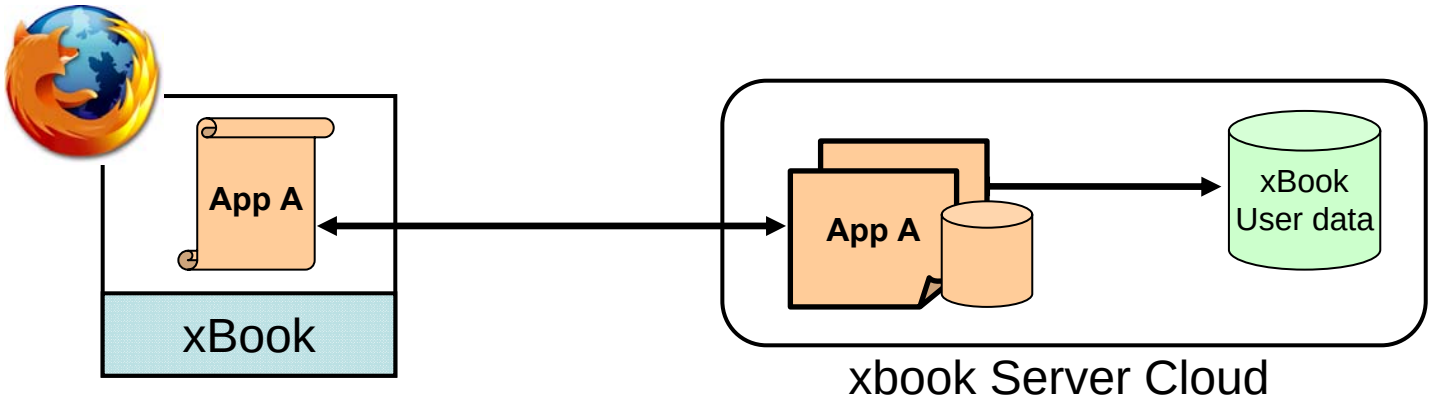
- Pull the applications into the trusted xBook domain.
- Monitor the applications at runtime in the browser.
- Allow applications access to any user data, but *require* them to make use of that data explicit.
- Use information flow techniques to prevent data leaks by the applications.

xBook Architecture



xBook platform divided into client-side and server-side.

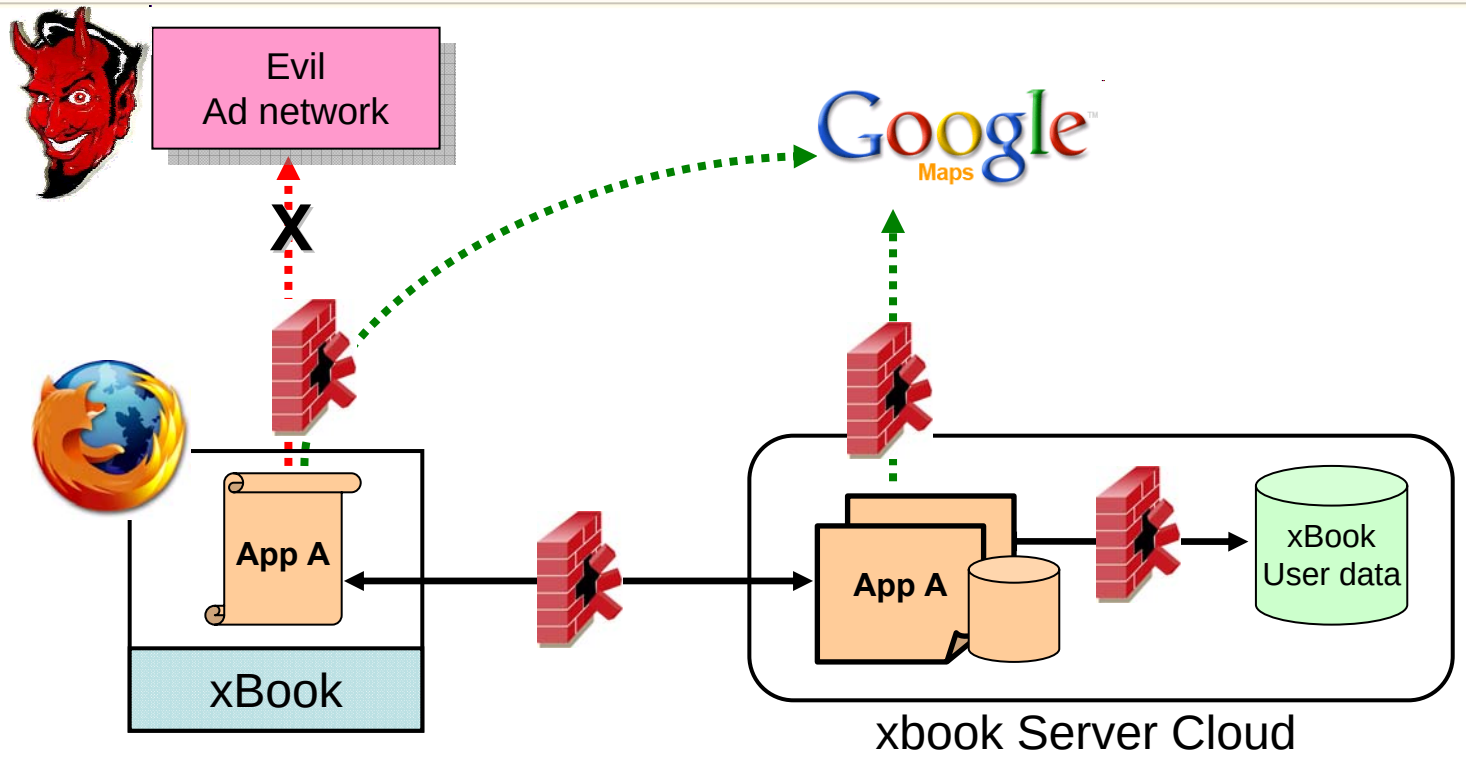
xBook Architecture



xBook platform divided into client-side and server-side.

An application is split into multiple components.

xBook Architecture



xBook platform divided into client-side and server-side.

An application is split into multiple components.

xBook mediates all component communication.

xBook Application Design

User profile

Example Application

- Complete user information to create customized profile.

xBook Application Design

Example Application

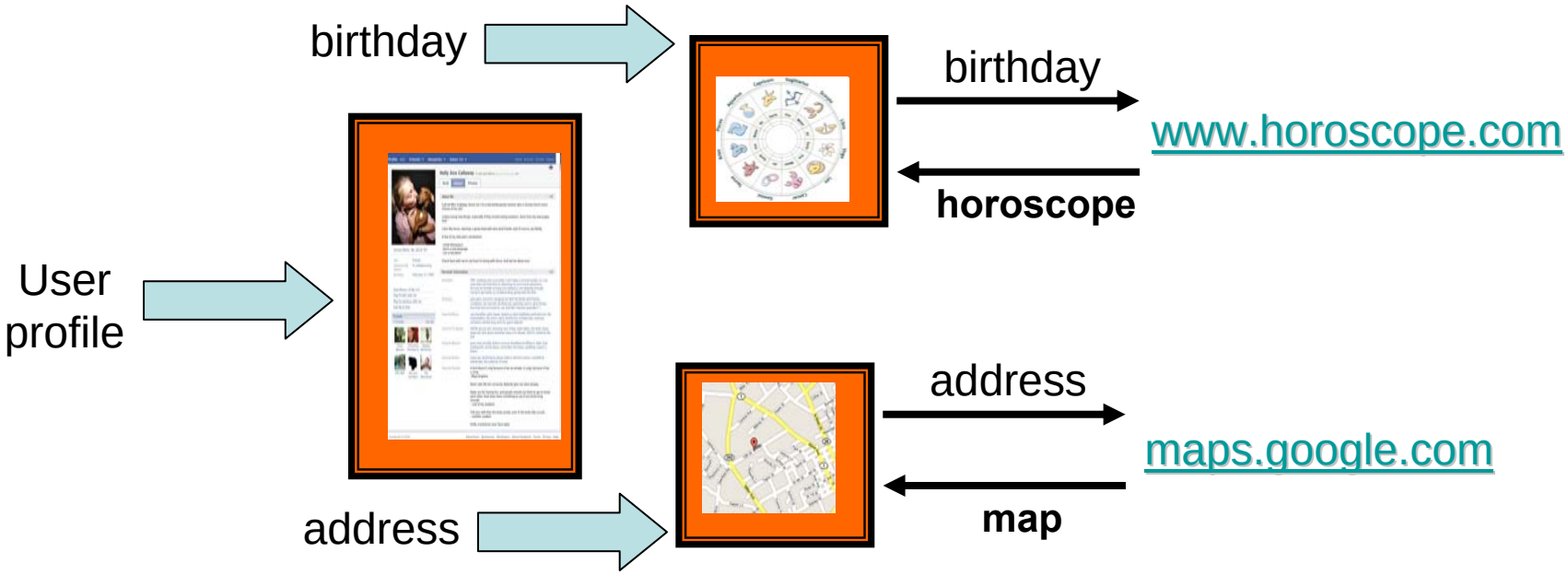
- Complete user information to create customized profile.
- Birthday to generate daily horoscope.

xBook Application Design

Example Application

- Complete user information to create customized profile.
- Birthday to generate daily horoscope.
- Address information to generate map.

xBook Application Design



Example Application

- Complete user information to create customized profile.
- Birthday to generate daily horoscope.
- Address information to generate map.

Application Lifecycle

Component	Data	External Entity
C0	<none>	-
C1	birthday	www.horoscope.com
C2	full profile	<none>
C3	address	maps.google.com

Information provided by application

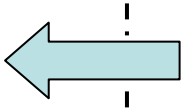
User's view

xBook view

Application Lifecycle

Data	External Entity
birthday	www.horoscope.com
address	maps.google.com

Application's manifest



Component	Data	External Entity
C0	<none>	-
C1	birthday	www.horoscope.com
C2	full profile	<none>
C3	address	maps.google.com

Information provided by application

User's view

xBook view

Application Lifecycle

Data	External Entity
birthday	www.horoscope.com
address	maps.google.com

Application's manifest

Component	Data	External Entity
C0	<none>	-
C1	birthday	www.horoscope.com
C2	full profile	<none>
C3	address	maps.google.com

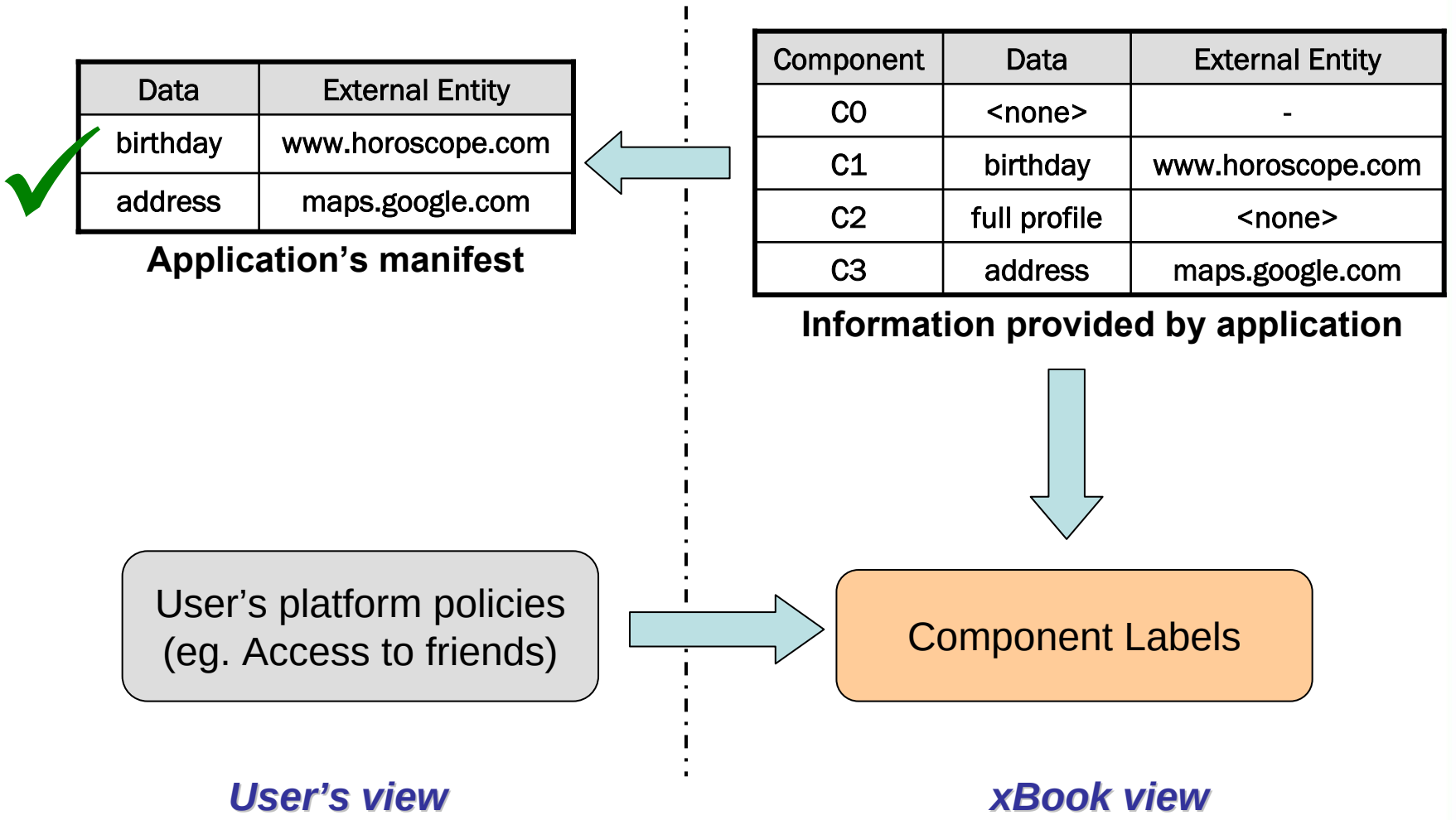
Information provided by application

User's view

xBook view

Georgia Tech College of Computing

Application Lifecycle



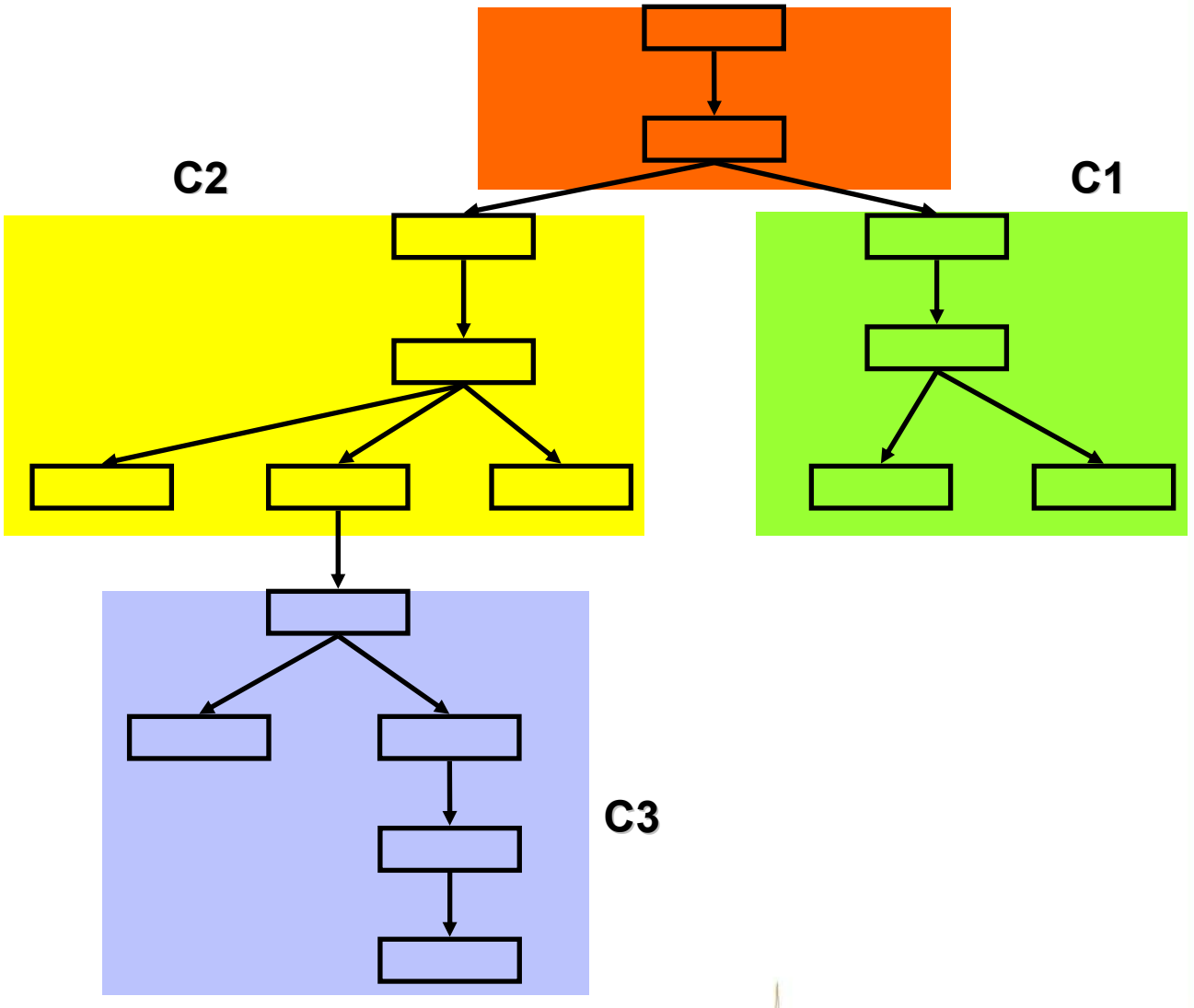


Client-side Confinement

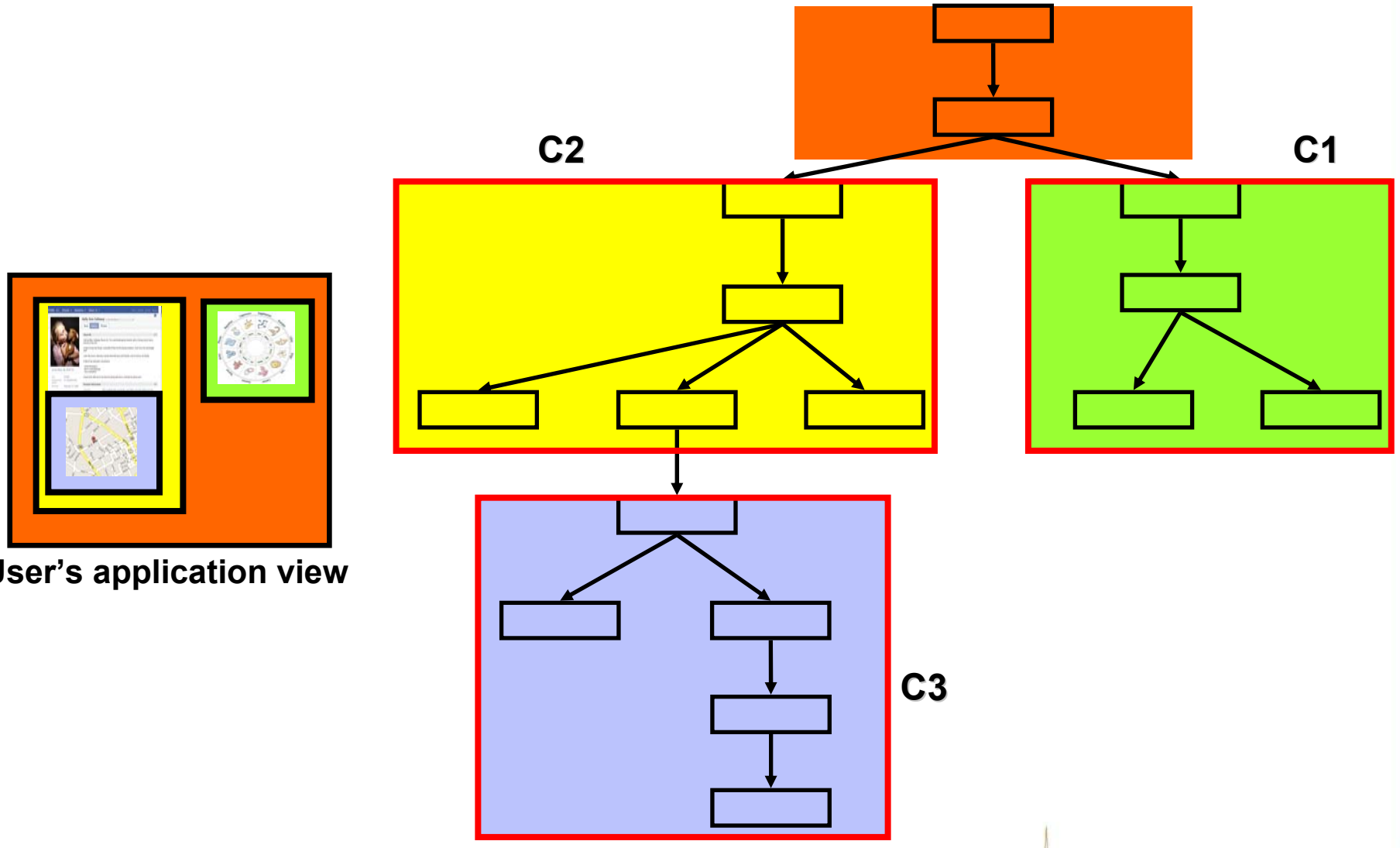
- Components written in ADsafe
  - ADsafe: Object capability subset of JavaScript
    - Unsafe JavaScript features like global variables, *eval*, etc. are removed from the subset.
  - Prevents the component from having direct access to the DOM elements of the page.
- Access is provided indirectly by providing a capability to the page services.

Client-side Confinement – DOM Isolation

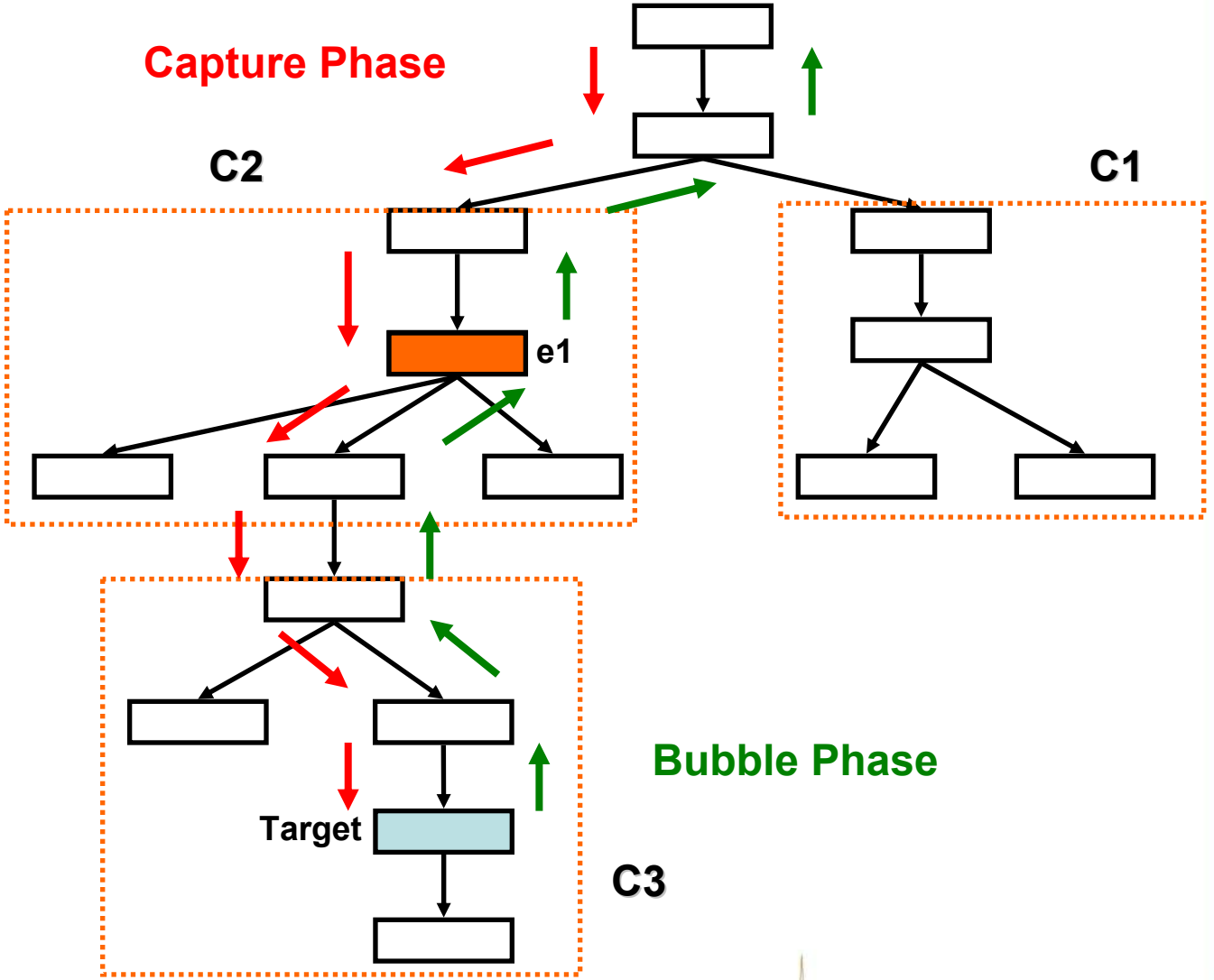
User's application view



Client-side Confinement – DOM Isolation

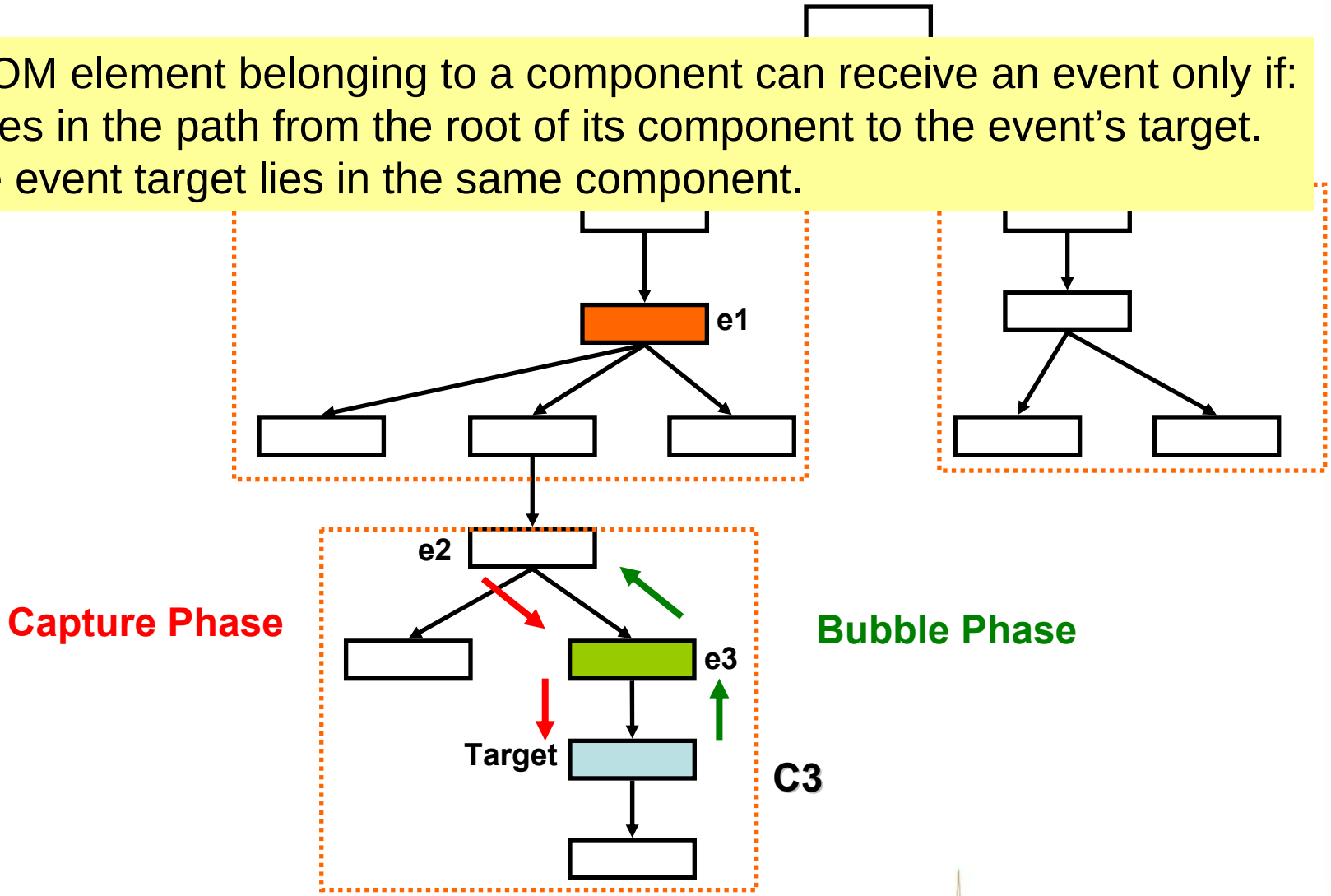


Client-side Confinement – EventListeners



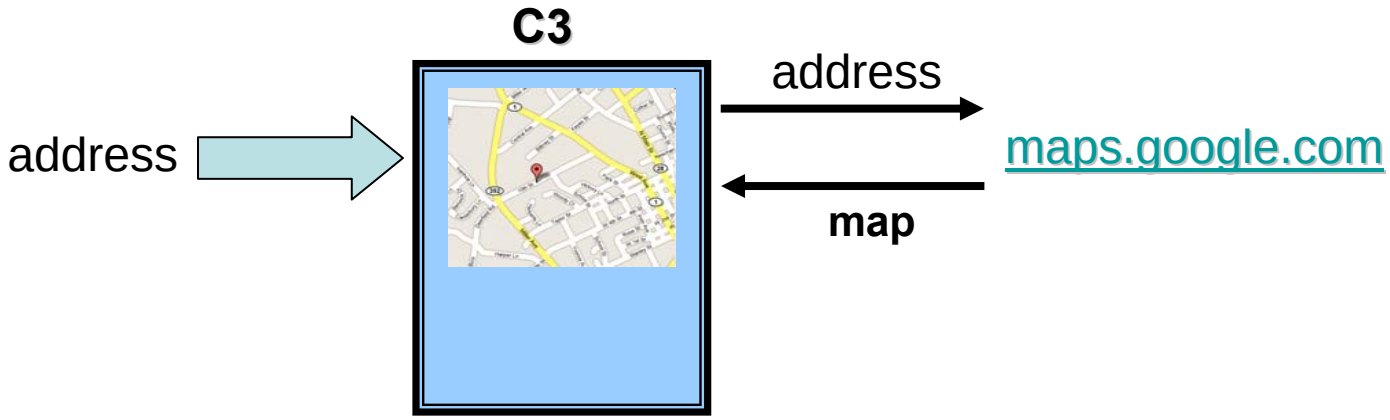
Client-side Confinement – EventListeners

A DOM element belonging to a component can receive an event only if:
- It lies in the path from the root of its component to the event's target.
- the event target lies in the same component.



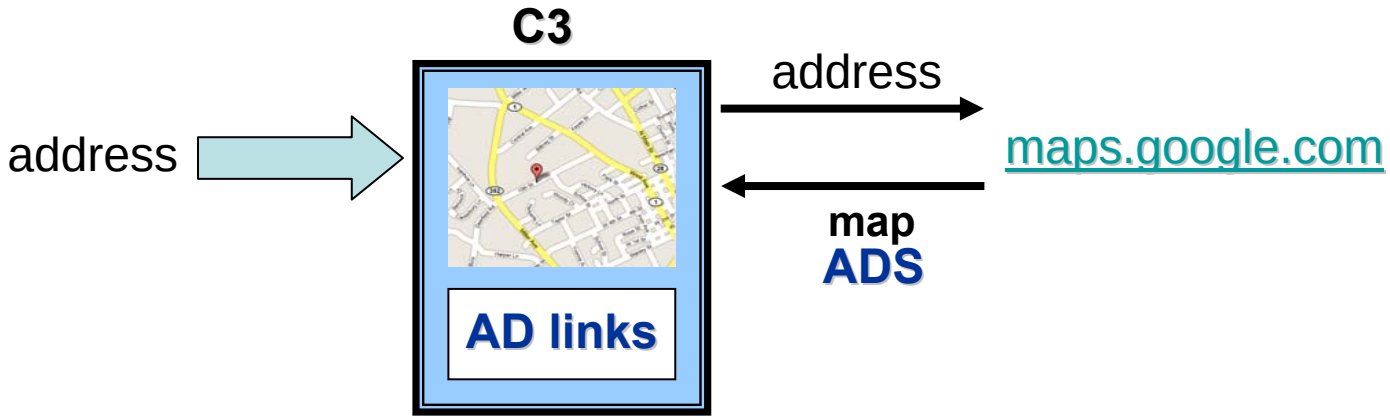
Communication with external entities

Symmetric communication



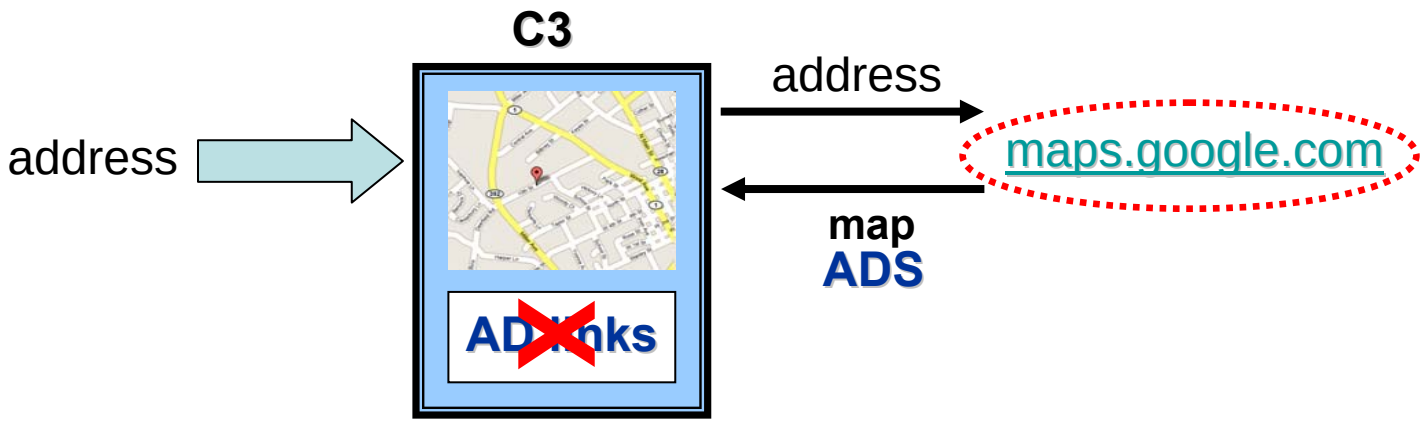
Communication with external entities

Symmetric communication



Communication with external entities

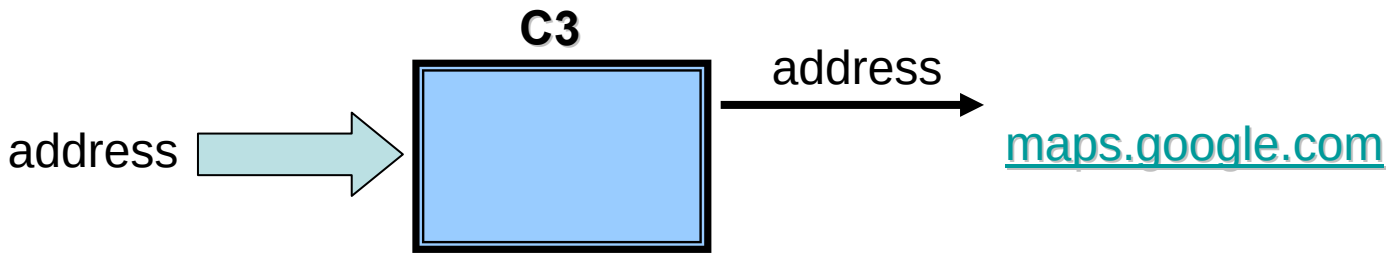
Symmetric communication



Problem: C3 cannot communicate with the Ad links.

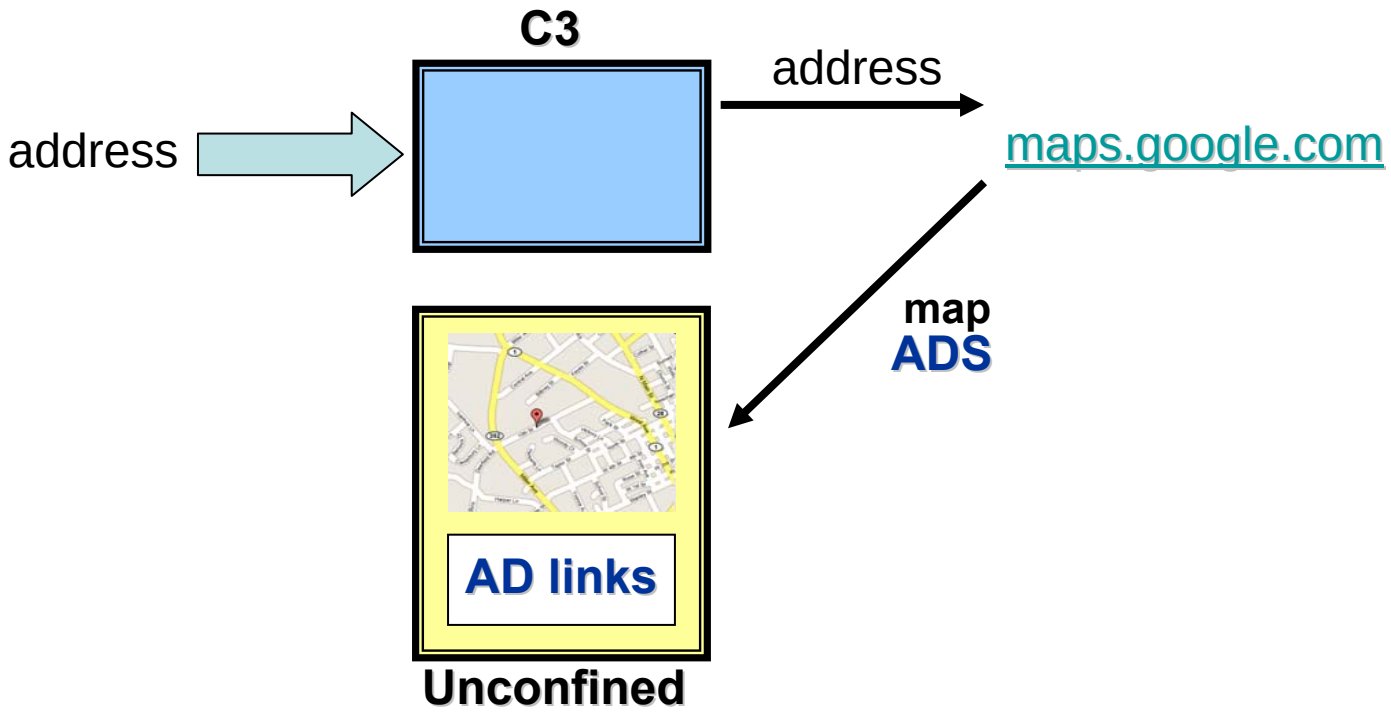
Communication with external entities

Asymmetric Communication



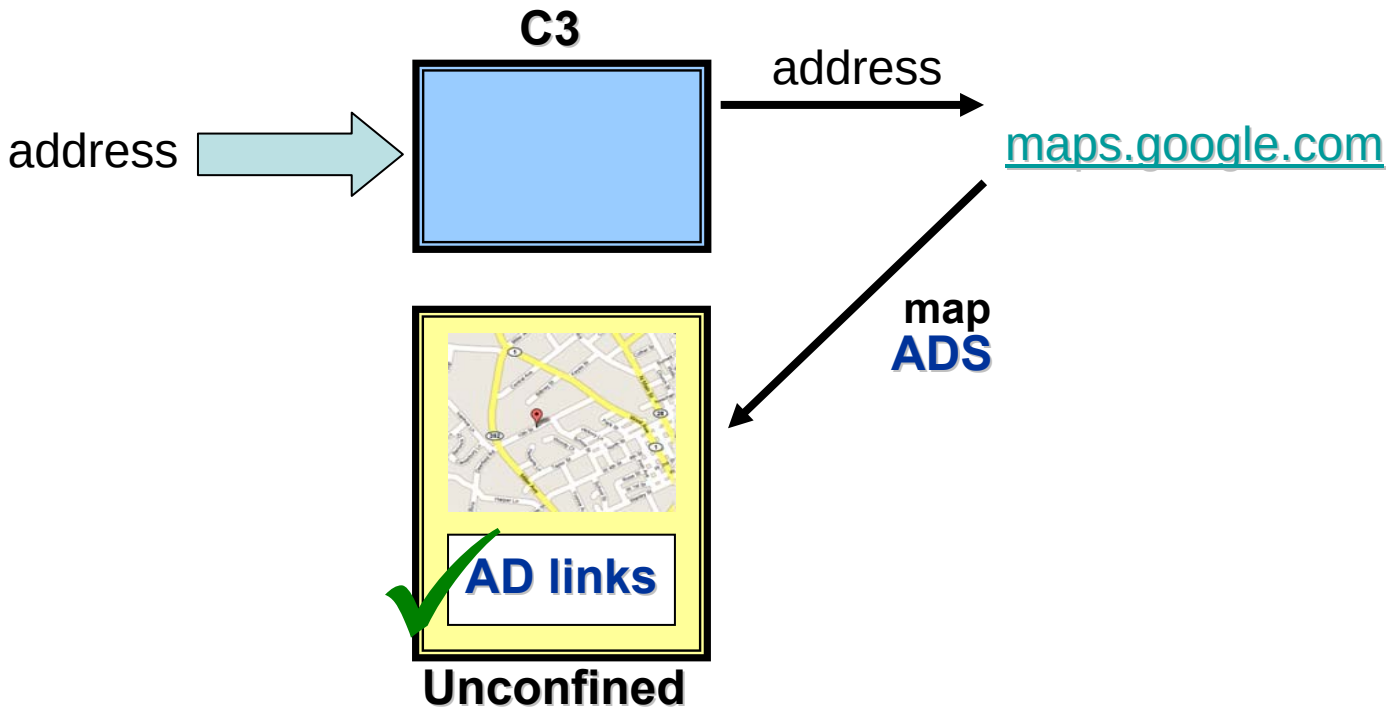
Communication with external entities

Asymmetric Communication



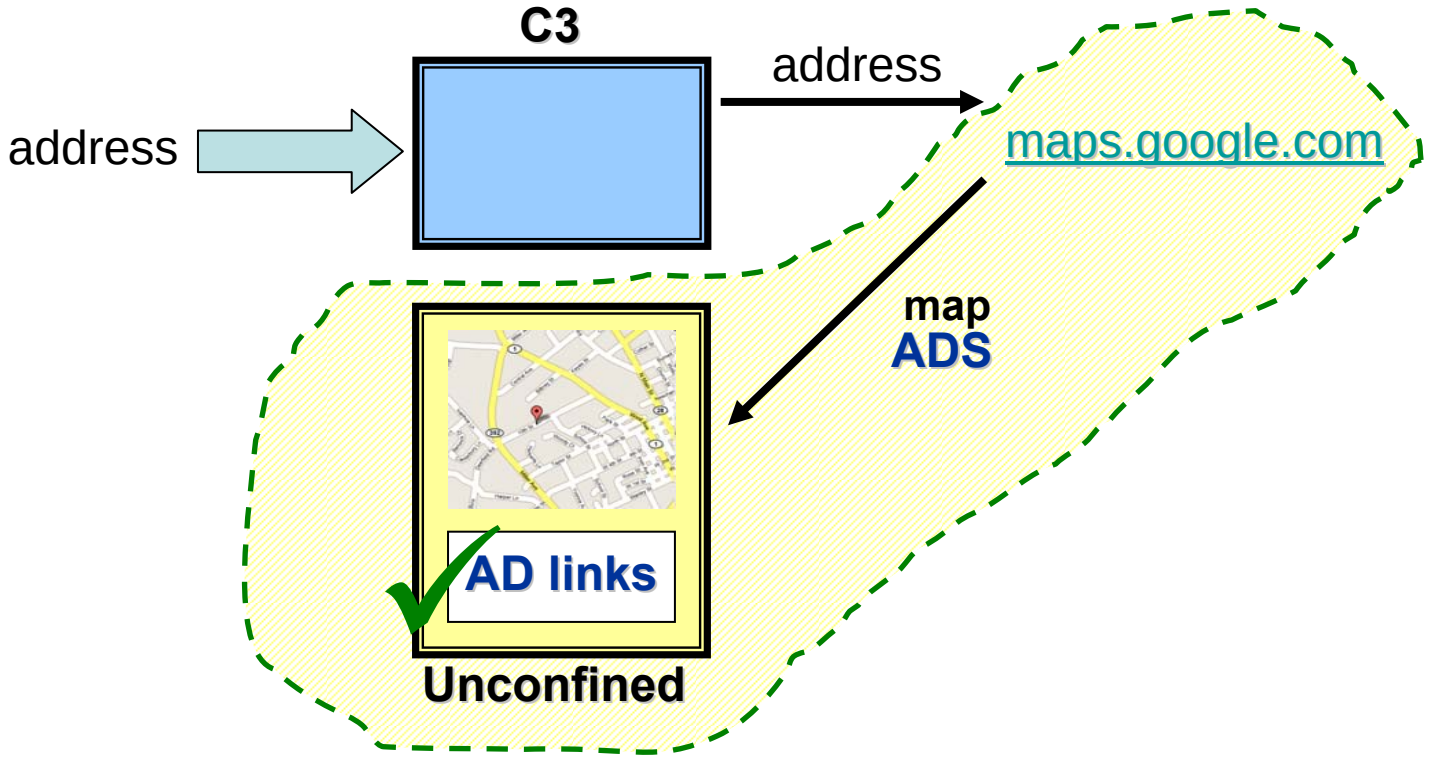
Communication with external entities

Asymmetric Communication



Communication with external entities

Asymmetric Communication





xBook on Facebook

- Ported xBook as an application on Facebook.
  - Facebook data feeds xBook's user data
  - Available at http://apps.facebook.com/myxbook
  - Users need to trust only xBook as an application



xBook on Facebook

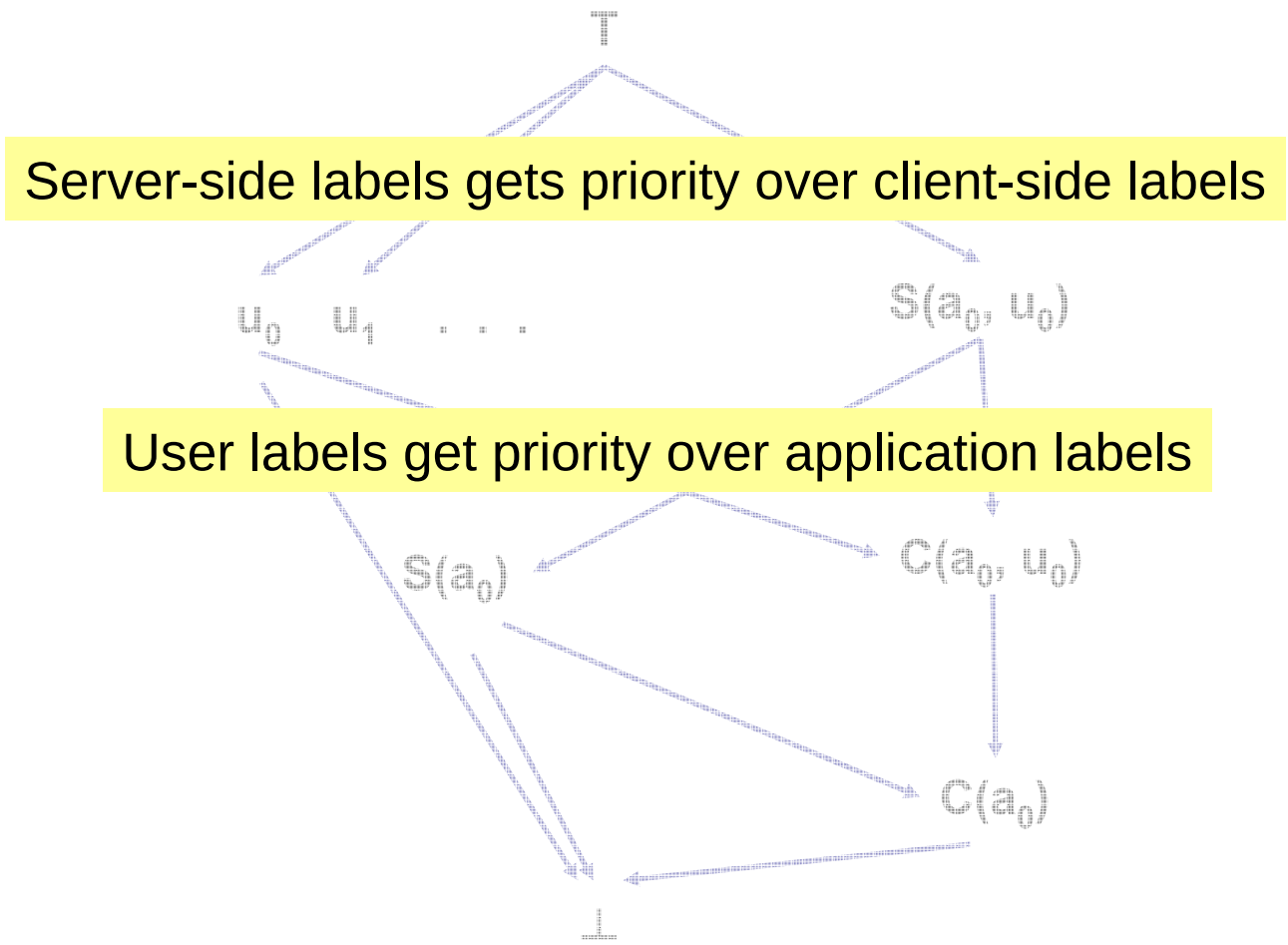
- Ported xBook as an application on Facebook.
  - Facebook data feeds xBook's user data
  - Available at http://apps.facebook.com/myxbook
  - Users need to trust only xBook as an application
- Incentives for application developers
  - User attraction: Applications developed over xBook provide greater privacy guarantees!
  - Future potential: Porting xBook as an application on any social networking platform will automatically port all xBook applications.



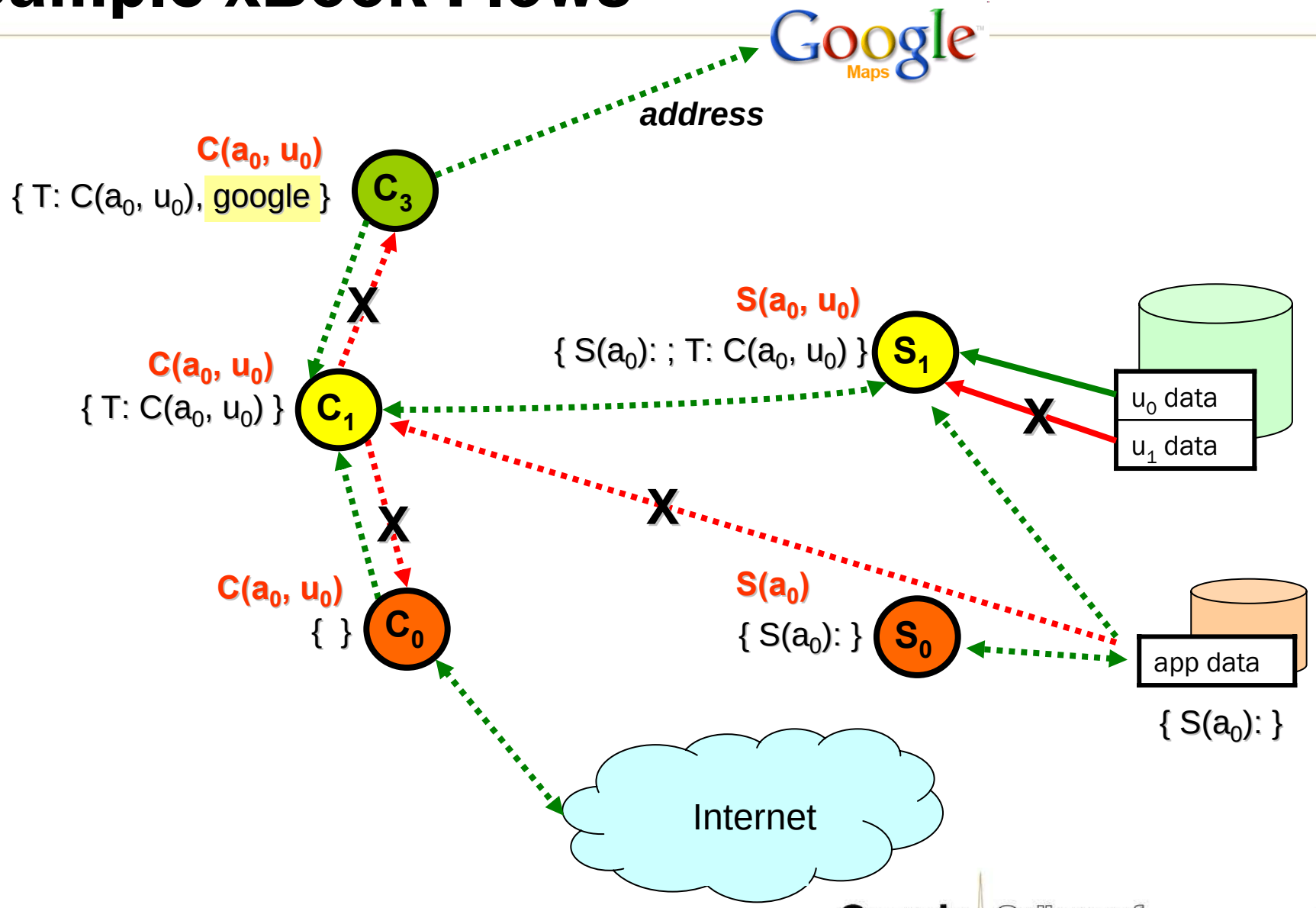
Applications

- xBook provides APIs for development of third party applications
  - developed two sample applications to show the applicability of the APIs.
  - Overhead: 4.2% (horoscope), 3.1% (utility application)

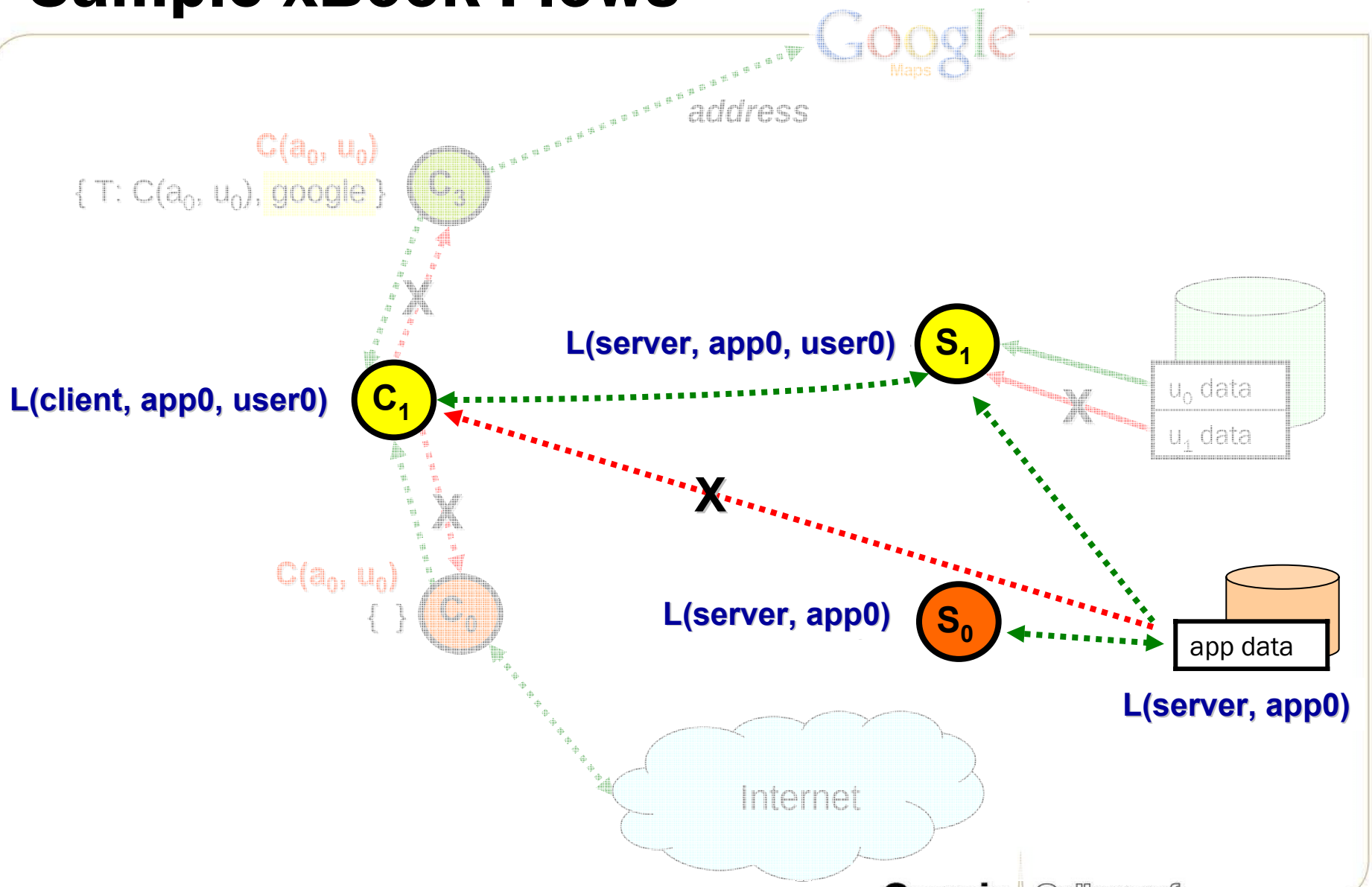
The Labeling System: acts-for hierarchy



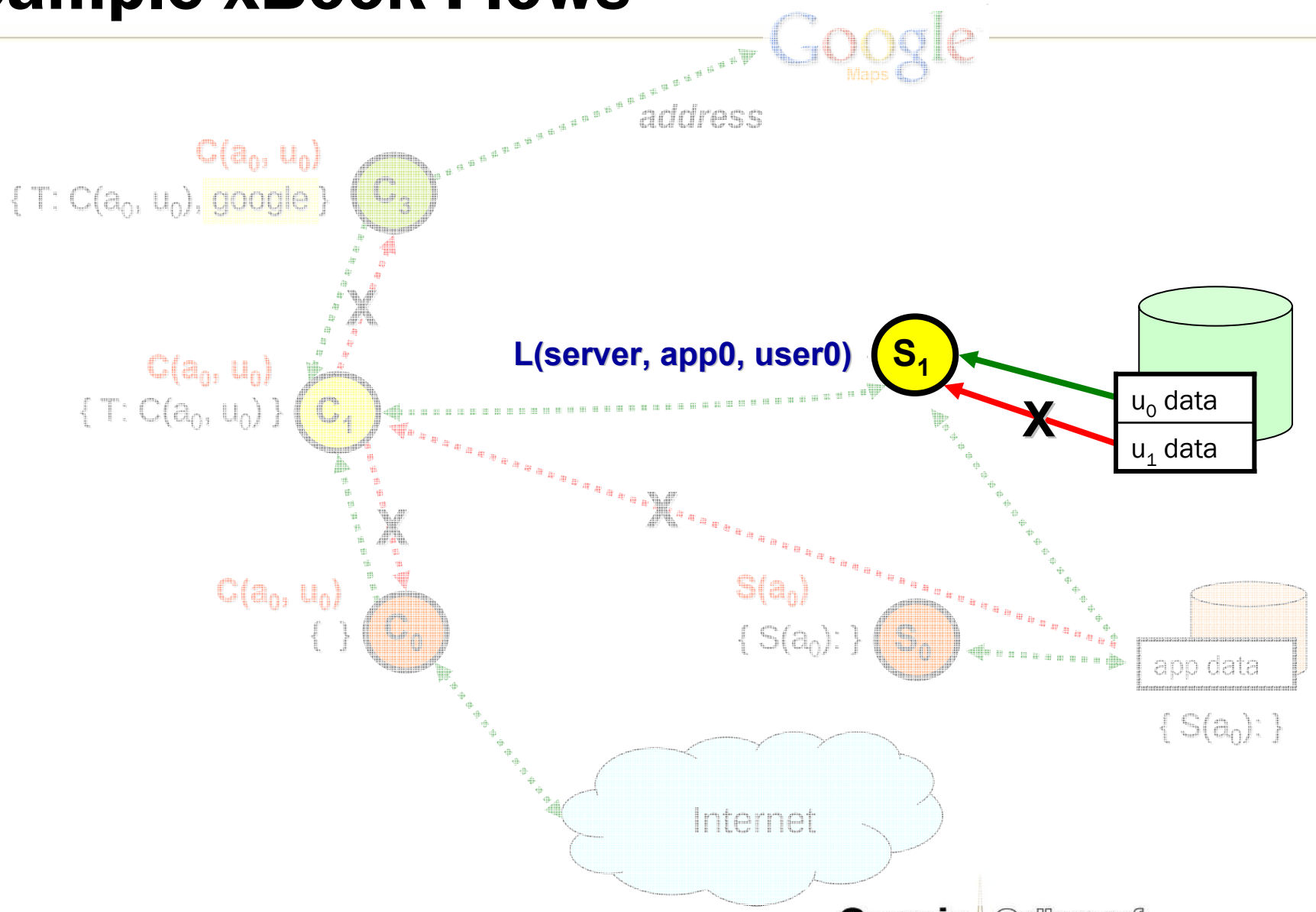
Sample xBook Flows



Sample xBook Flows



Sample xBook Flows





Conclusions

- Presented a novel framework for improving user privacy in social networks in view of third party applications.
- xBook allows applications to have access to any user data, while still preventing them from leaking the data.
- A working prototype of the xBook system was developed and is available online.
- Set of APIs are available for developing xBook applications.



Thank You.

Questions?

ksingh@cc.gatech.edu