1/12/2012

Secure Personal Content Networking over Untrusted Devices

이 의 진

uclee@kaist.ac.kr

KAIST 지식서비스공학과

공동연구: Josh Joy, Mario Gerla (UCLA CS)
Jihoon Ahn (KAIST CS)

HSN 2012
The 22nd High-Speed Network Workshop
Human-Centric Networking for The Future
2012. 1. 11(수) ~ 13(금) | 제주 그랜드 호텔

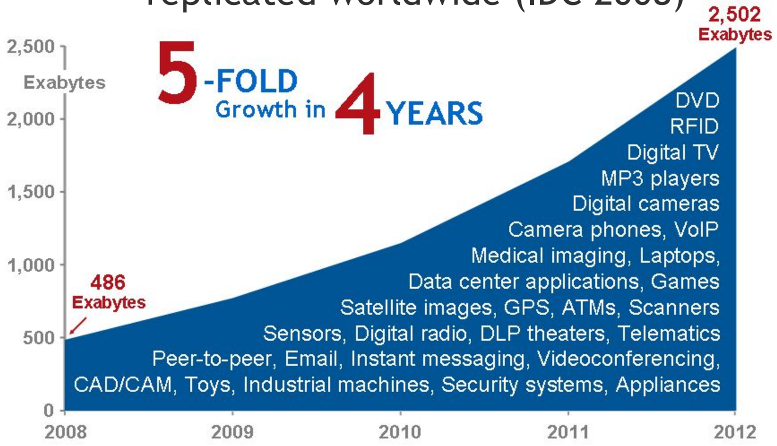
KAIST
한국과학기술원

Motivation

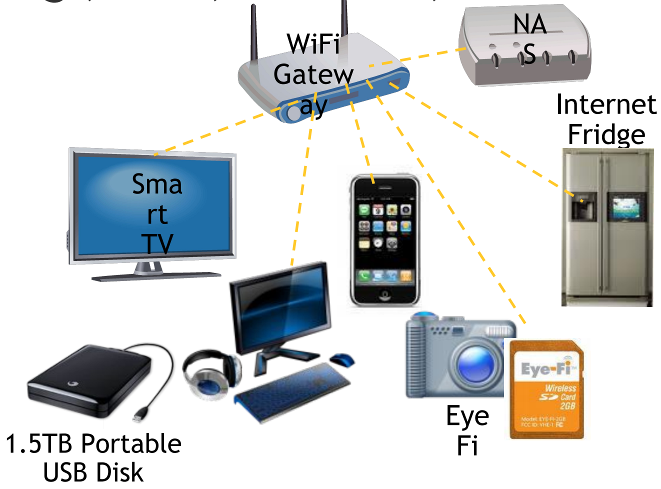
# personal devices are increasing (so does the data in/generated by them)

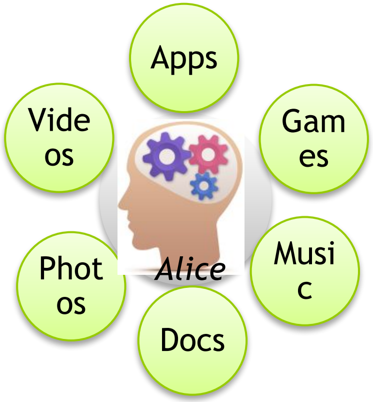
- Smartphones, cameras, smart-home devices (e.g., Internet fridges/TVs, etc)
- Often have Internet connection capability via different forms of communications: e.g., WiFi, Ethernet, Bluetooth, 3G/LTE

Digital information created, captured, replicated worldwide (IDC 2008)



Source: IDC Digital Universe White Paper, 2009





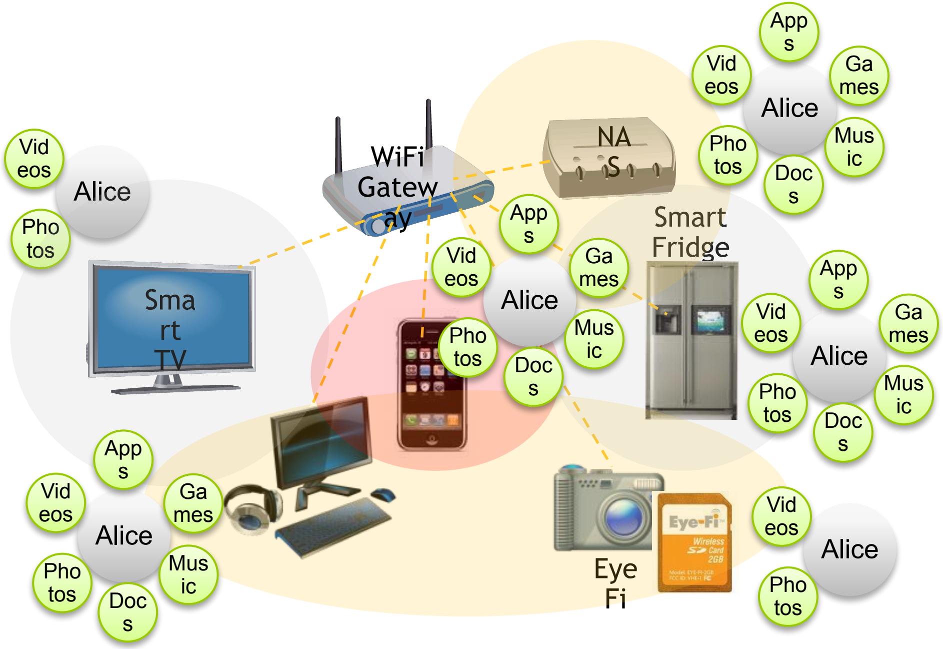
Mental Model:
Personal Document Space (PDS)*

**Personal Information Management, William Jones Annual Review of Information Science and Technology, Volume 41, Issue 1, pages 453-504, 2007*

Motivation

Yet, accessing/managing/sharing content over these devices is still challenging:

- Heterogeneous devices/vendors/protocols
  - Zero-configuration/unified content access platform is a must (for non-techy persons)
- Management of content over multiple devices is laborious
- Selectively sharing content among friends is still hard

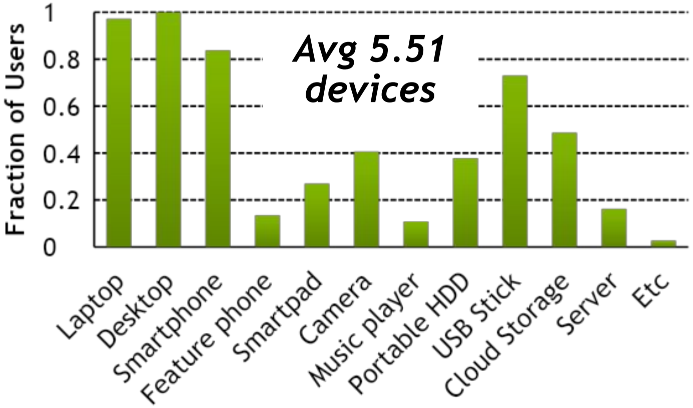


Motivation: Content Management Practices

Interview study of 37 users (30 males, 7 females, mostly graduate students):

(1) device collection?

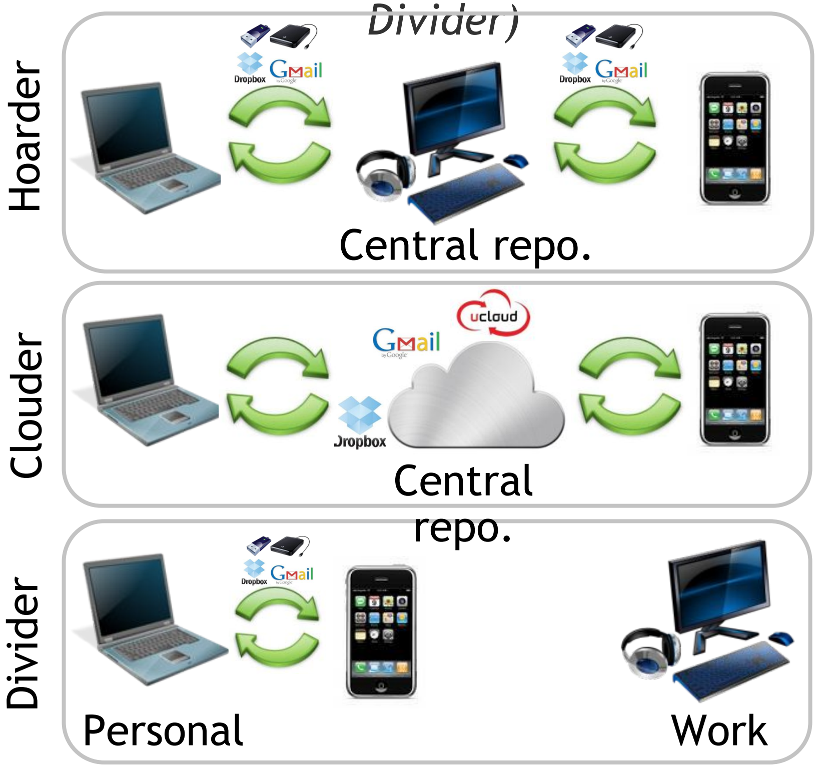
(2) content management practices?



Device Collection

Content Management Patterns

(Don't-carer, Hoarder, Clouder, Divider)

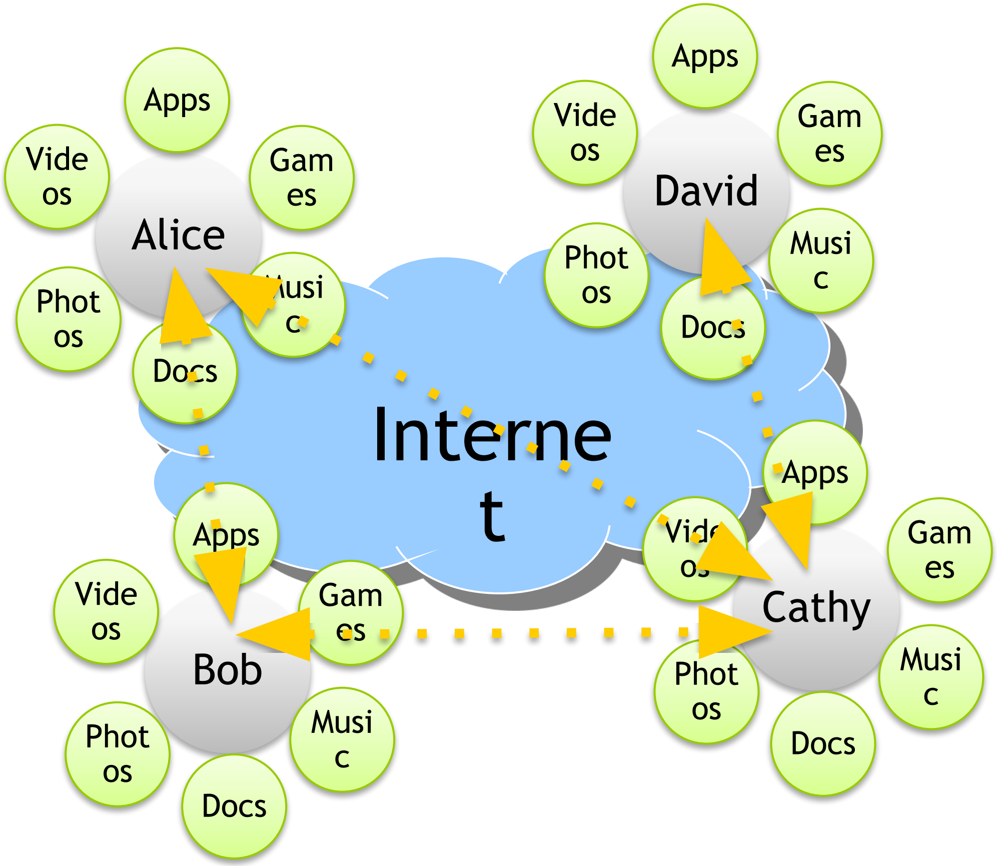


Sync is difficult: downloading/sharing content happens everywhere (including UCG content)

Cloud storage can't store all the user data (limited capacity; economically not feasible)

Personal/work boundary is not always crystal clear; often blurred over the period of time

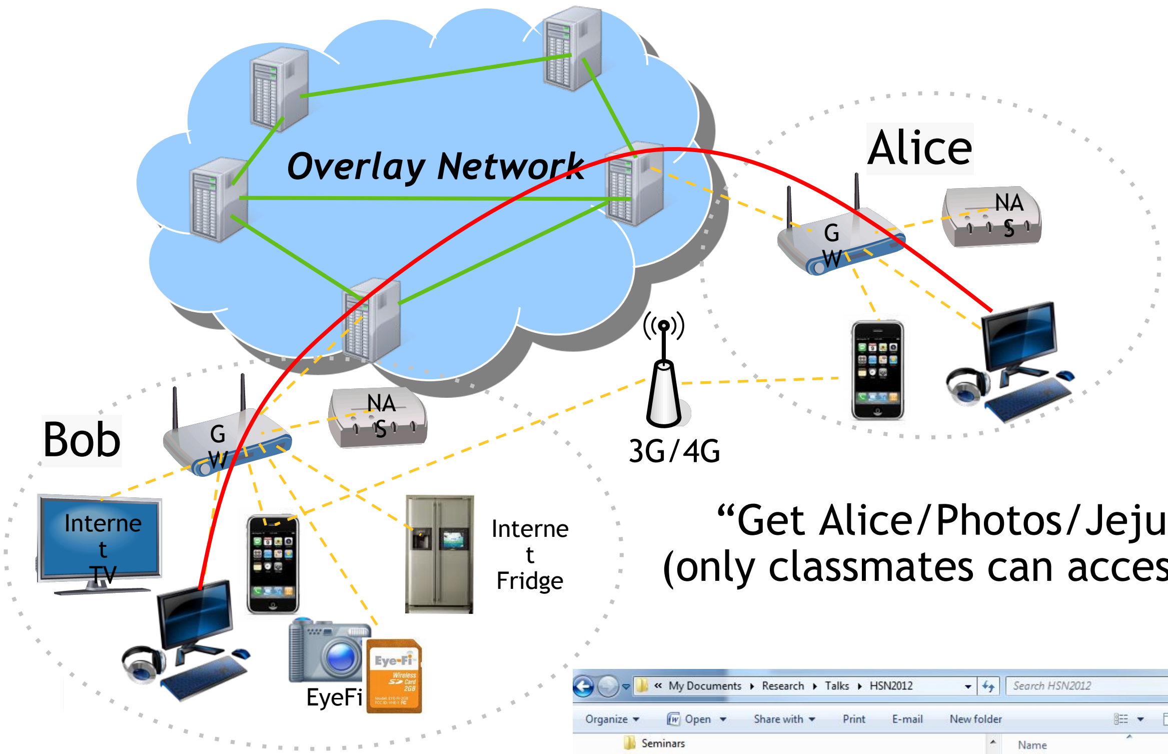
Towards Personal Content Networking (PCN)

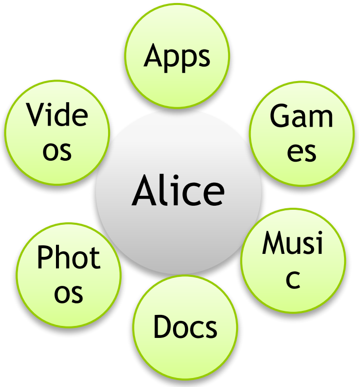


PCN Wish list

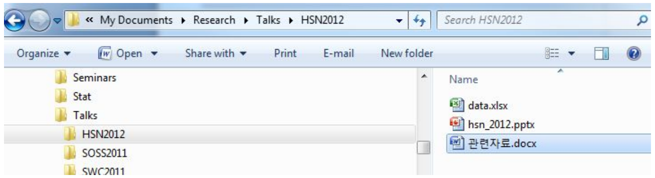
- Single persistent, hierarchical namespace of personal content
- Full control of content management (control of every personal storage, **including cloud storage**)
- Selective content sharing among friends (fine-grained access control)
- Disrupted operations
- Security/privacy guarantee

Personal Content Networking (PCN)





“Get Alice/Photos/Jeju2012.jpg”
(only classmates can access this photo)



PCN extends **Content Centric Networking (CCN)** platform to support **selective content sharing** and **seamless distributed content management**

Related Work: Distributed File Systems and Beyond

		Naming	Disruption	Topology	Replica Unit	Update	Trust Mgt	Access Control	Secure Binding
Mobile DFS	Ficus	SP+H	Yes	P2P	Volume	Yes	-	ACL	-
	Coda/BlueFS	SP+H	Yes	C/S	File	Yes	-	ACL	-
Pervasive FS	UIA/Eyo	DP+H	Yes	P2P	-	-	PKI	ACL	-
	PersonalRAID	SP+H	Yes	P2P	Volume	-	-	-	-
	Footlose	SP+F	Yes	P2P	File	-	-	-	-
Semantic FS	HomeView/ Perspective	Semantic	Yes	P2P	View	-	-	-	-
Crypto FS	Plutus/SiRiUS	SP-H	No	P2P	C/S	-	PKI	Certs/PKC	-
P2P FS	PAST/CFS	SP+F	No	P2P:DHT	File Bloc				
Future Internet	CCN	SP+H	Yes						
	PCN	SP+H	Yes	P2P	File	Yes	Yes	Certs/ABAC	Yes

+ Secure Binding
+ Content Caching

+ Consistency/Content Management (Read-Write)
+ Fined-grained content centric access control

SP/DP (single persistent/device persistent); F/H (flat/hierarchical) structure

IBAC (Identity-based Access Control; e.g., ACL); ABAC (Attribute Based Access Control; e.g., ABE)

Toward Secure Personal Content Networking

1. **Naming convention**: single persistent namespace of personal content

2. **Trust management**: SPKI/SDSI based principal introduction (key distribution)

3. **Overlay network**: to facilitate data sharing among friends

4. **Content centric networking (CCN)**: content can be accessed by name

- Any host that has the requested content will serve the content

5. **Content centric access control for selective content sharing**:

- Attributed Based Encryption (ABE) for decentralized access control

6. **Content management**: managing content (e.g., replicating/removing/migrating content) over multiple devices

7. **Content update and consistency management**: updating content and preserving consistency of content (eventual consistency)

Namespace of Personal Content

SPKI/SDSI style naming:

- Principal ID (PID): Alice names herself **PID = {P_Alice Alice}** (P_Alice = pub key)
- Hierarchical naming is possible
  - Example: “**K_0** kaist hs_eng cs uichin” (recursive definition a la DNS)

Apps
Videos
Games
Photos
Alice
Music
Docs

PID = {P_Alice Alice}

{P_Alice Alice}/photos/hsn.jpg

Personal address book (local name resolution)

- Introduction allows users to securely distribute public keys
- After introduction process, one can create a local mapping:
  - Human readable name to PID
  - Note that *UIA is “host centric”: name is given to a device (not a principal)

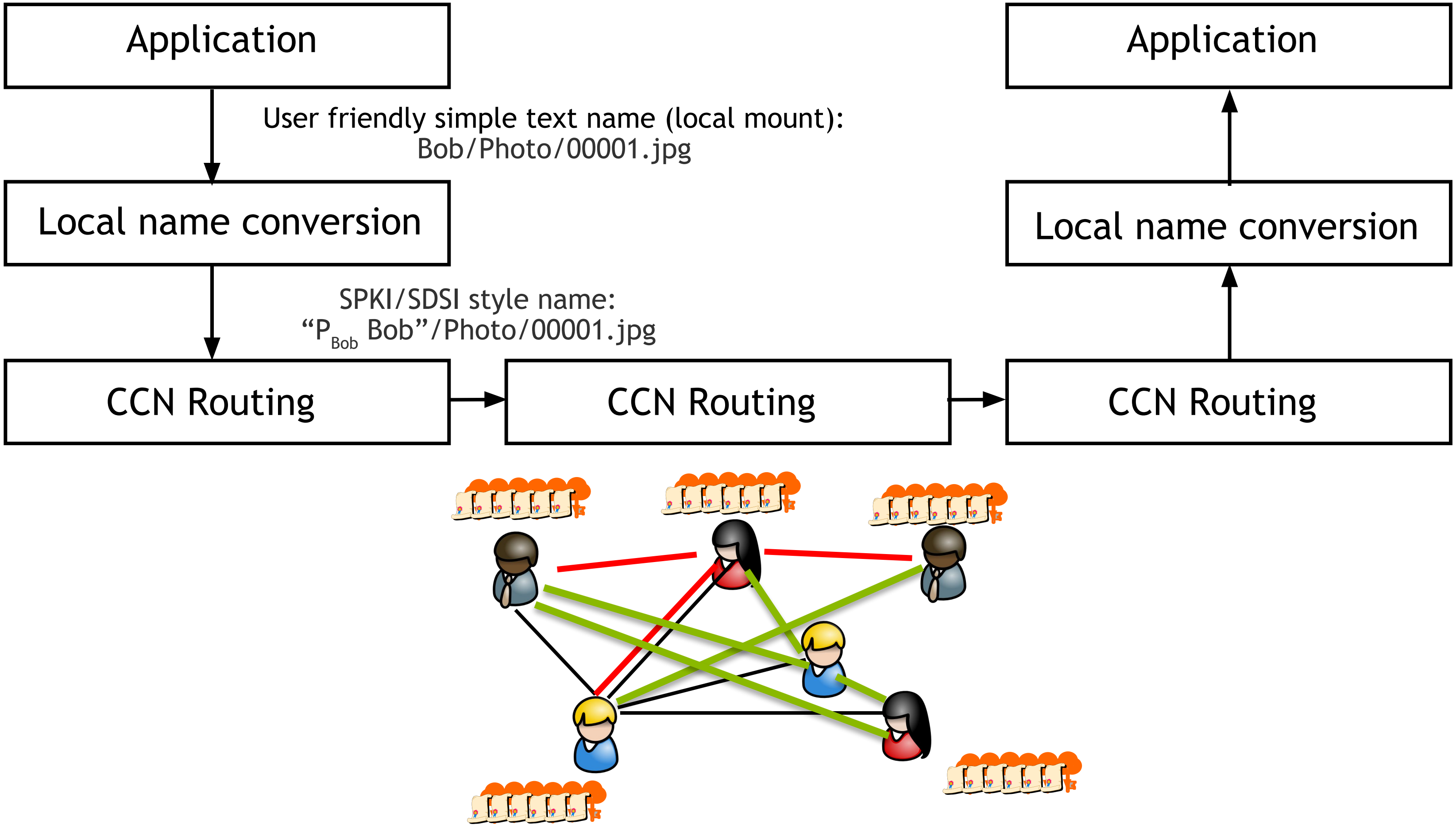
Content naming: N = {PID + Label}

- “Label” is personal content name space (DONA style)
- Secure binding of content C with name N as in CCN: Sig(N, D)

*Persistent Personal Names for Globally Connected Mobile Devices, Bryan Ford et al., OSDI 2006

Content Routing (Overlay)

Overlay network based on social networks



Application

User friendly simple text name (local mount):
Bob/Photo/00001.jpg

Local name conversion

SPKI/SDSI style name:
“P_{Bob} Bob”/Photo/00001.jpg

CCN Routing

CCN Routing

CCN Routing

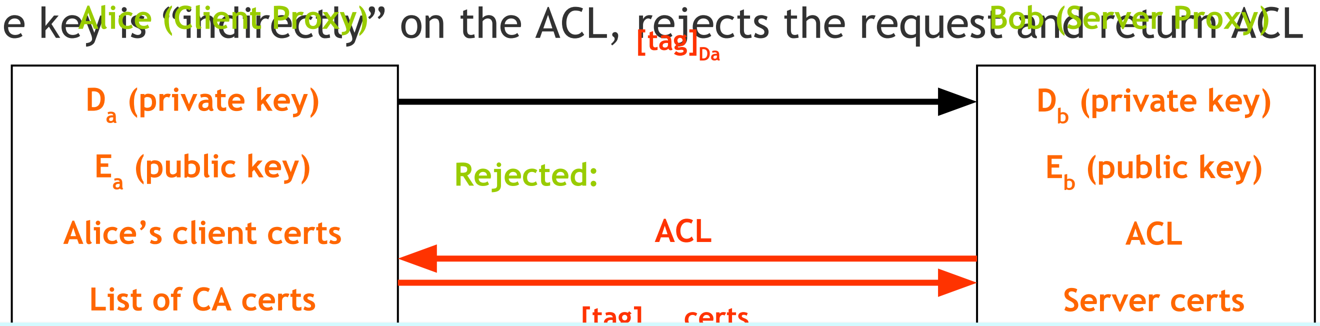
Local name conversion

Application

Content Centric Access Control

Limitation of SPKI/SDSI's access control

- SPKI/SDSI only provides a host centric access control
  - Need to secure "channel" for secure access control
- How it works?
  - Initialization: set up SSL connection between two hosts (client and server)
  - if a requester's key is directly on the ACL of the server, granted!
  - if the key is "indirectly" on the ACL, rejects the request and return ACL (below)



Host-centric access control (trusted server)

□□

Not applicable to distributed CCN env. w/ content caching
(any untrusted intermediate node can peek into cached content)

Content Centric Access Control via CP-ABE

Wish-list for PCN:

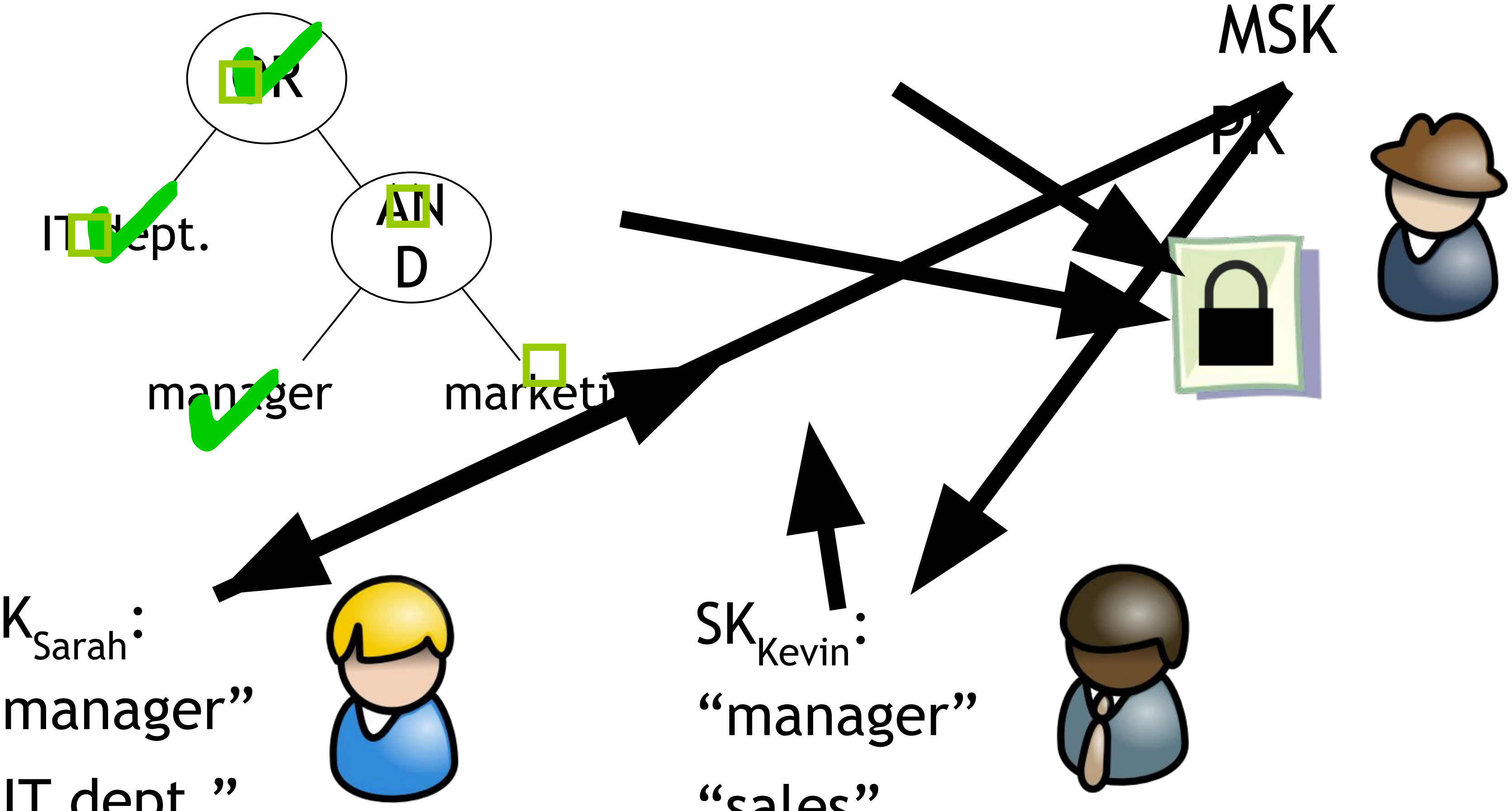
- Encrypted files for untrusted storage (*caching* in the intermediate routers)
- No online, trusted centralized third party mediating access to files or keys
- Highly expressive, fine grained access policies

Ciphertext-policy attribute-based encryption (CP-ABE) does this!

- User private keys given list of "attributes"
- Files can be encrypted under "policy" over those attributes
- Can only decrypt if attributes satisfy policy

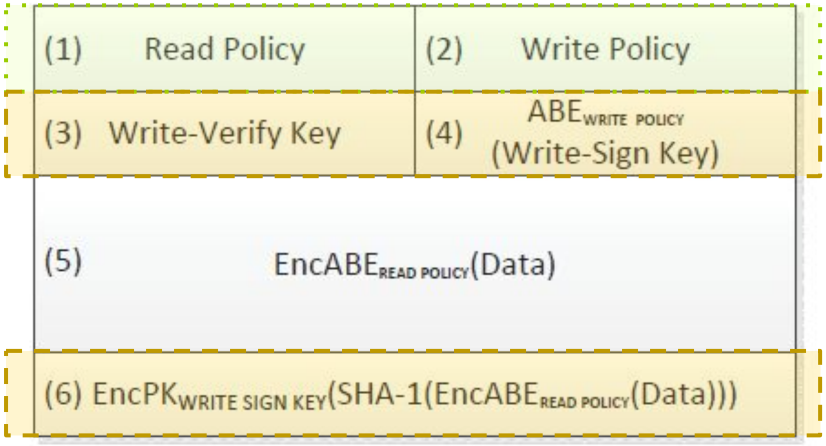
Content Centric Access Control via CP-ABE

MSK: Master Secret Key
SK: Secrete Key (Private Key)
PK: Public key



Content Centric Access Control via CP-ABE

PCN File Header



(1) Read Policy	(2) Write Policy
(3) Write-Verify Key	(4) $ABE_{WRITE\ POLICY}$ (Write-Sign Key)
(5) $EncABE_{READ\ POLICY}$(Data)	
(6) $EncPK_{WRITE\ SIGN\ KEY}$(SHA-1($EncABE_{READ\ POLICY}$(Data)))	

Users can define <u>read and write policy</u> (for each file)

Only users w/ <u>valid write-access authorization</u> can update files

Replica Updates

Our goal:

- Eventual consistency: all updates are eventually propagated to all replica
- File-level consistency (like FICUS)

Supporting “update” via augmented prefix announcement

- Updated replica contains extra metadata (version vector)
- Prefix announcement with “modification mark” and “updated location”
  - Say “Bob/mydoc/test.doc” was updated
  - **Announced prefix** is “Bob/mydoc” and **updated location** is “Bob/mydoc/test.doc”

PCN supports prefix protection (as in S-BGP)

Attribute based encryption support

- Modified content needs to be re-encrypted with ABE
- New version will be signed by the updater, and its prefix will be announced

Distributed Content Management

Device-to-device communication via reserved common name space (as in UNIX device files):

- Alice’s iphone talks to ipad:
  - Alice:/dev/iphone, /dev/ipad/

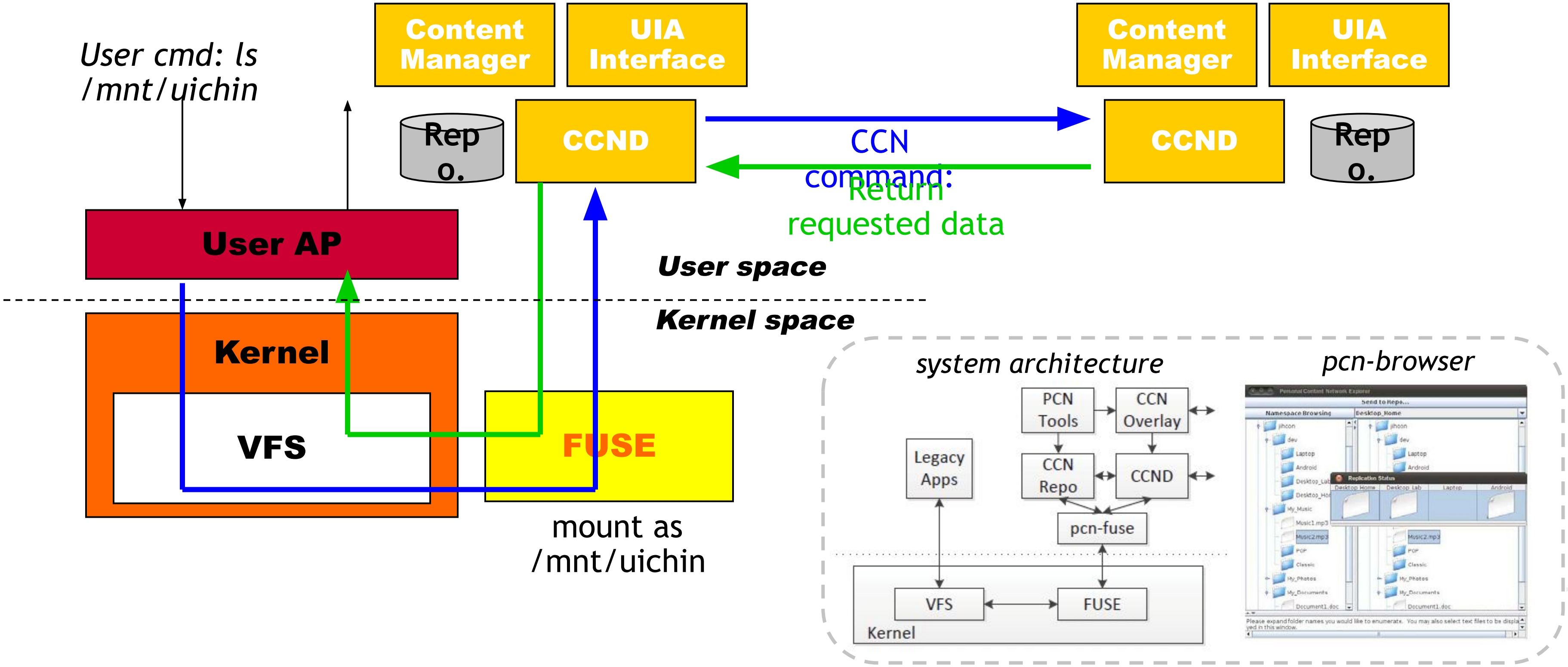
Sending content management commands to specific devices

- Update a special script file (called .cmd) in the target device directory
  - Example: copying files to my iPad □ a list of files to be copied is placed in /dev/ipad/.cmd, and file update is notified via prefix announcement
  - My iPad will receive the announcement, and the command file will be fetched and executed

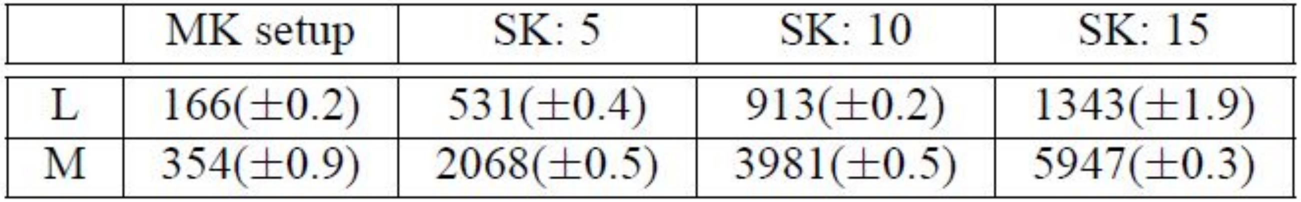
Prototype Design: FUSE + CCN

Providing a transparent view of the content available on the CCN network

- FUSE: a user level file system
- CCND is augmented with FUSE VFS operations (e.g., open, write, etc.)
- Mounting person’s namespace (e.g., /mnt/uichin)



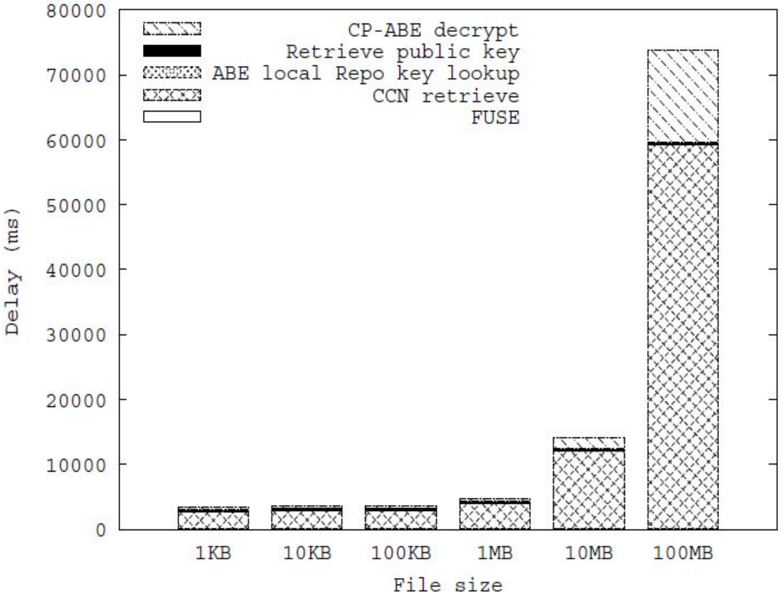
Preliminary Evaluation



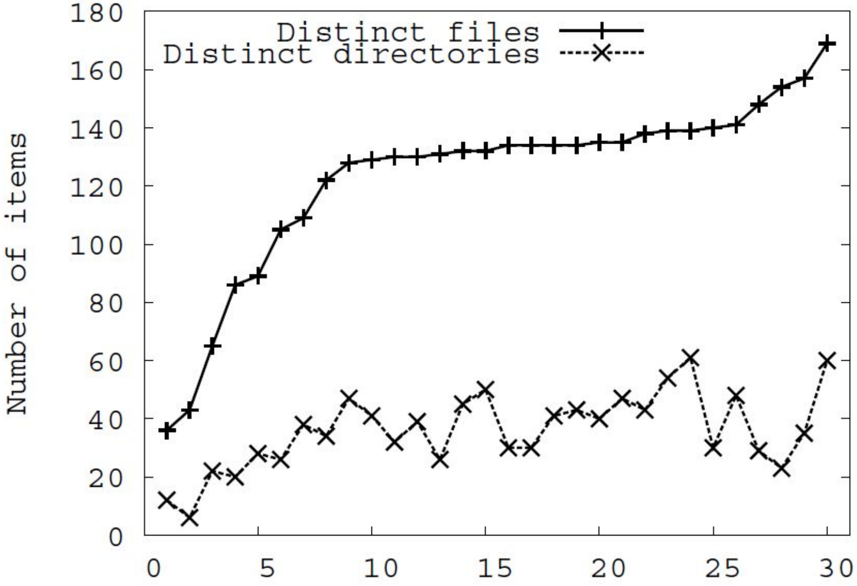
	MK setup	SK: 5	SK: 10	SK: 15
L	166(±0.2)	531(±0.4)	913(±0.2)	1343(±1.9)
M	354(±0.9)	2068(±0.5)	3981(±0.5)	5947(±0.3)

CP-ABE performance of Laptop (L) and Nexus One (M) in milliseconds: master key (MK) setup and secret key (SK) generation with *k number of attributes*

□ ***attribute generation takes time, but it's one-time setup cost***



Remote file retrieval with ABE (Laptop)



Recently accessed files and directories (user traces) □ ***small routing table size***

Summary

Extended CCN to realize personal content networking (PCN)

- Single persistent namespace of personal content
- Securely initialize devices and establish trust relationship among users
- Social network based overlay network for CCN content delivery
- Content centric access control via attribute-based encryption (ABE)
- Personal content management tool using persistent namespace
- Content update and consistency management
- Legacy application support via FUSE, a user level file system

Ongoing Work:

- Personal content management practice: longitudinal usage behavior monitoring
- Large scale testbed experiments using Amazon EC2 servers