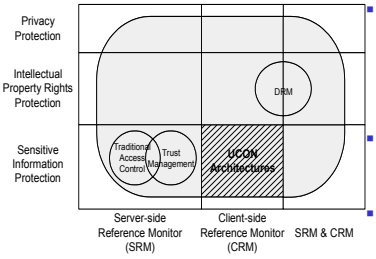
Usage Control Architectures

INFS767, Oct. 23, 2003

Ravi Sandhu and Jaehong Park
(www.list.gmu.edu)

Laboratory for Information Security Technology (LIST)
George Mason University

UCON Architectures

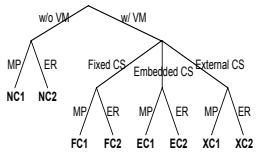


- We narrow down our focus so we can discuss in detail how UCON can be realized in architecture level
  - Sensitive information protection X CRM
- First systematic study for generalized security architectures for digital information dissemination
- Architectures can be extended to include payment function

Three Factors of Security Architectures

- Virtual Machine (VM)
  - runs on top of vulnerable computing environment and has control functions
- Control Set (CS)
  - A list of access rights and usage rules
  - Fixed, embedded, and external control set
- Distribution Style
  - Message Push (MP), External Repository (ER) style

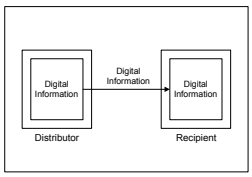
Architecture Taxonomy



VM: Virtual Machine
CS: Control Set
MP: Message Push
ER: External Repository

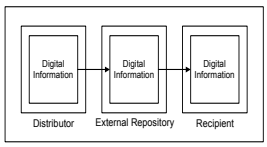
NC1: No control architecture w/ MP
NC2: No control architecture w/ ER
FC1: Fixed control architecture w/ MP
FC2: Fixed control architecture w/ ER
EC1: Embedded control architecture w/ MP
EC2: Embedded control architecture w/ ER
XC1: External control architecture w/ MP
XC2: External control architecture w/ ER

No Control Architecture w/ Message Push (NC1)



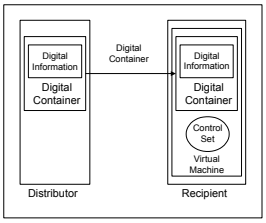
- Distributor directly sends a copy of digital contents to each recipient
- Each recipients stores the copy of digital information at local storage
- After distribution, no direct means to control the distributed digital information
- To access the digital information from multiple system, the recipient needs to transport the information

No Control Architecture w/ External Repository (NC2)



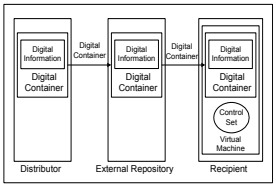
- Digital information is sent to an external repository server for distribution
- A recipient must connect to the external repository to access the digital content
- Once a recipient has received the digital contents, there is no way to control access or usage

Fixed Control Architecture w/ Message Push (FC1)



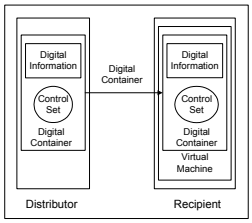
- Digital content is encapsulated in a digital container
- Control set is encoded into virtual machine
- The control set cannot be changed after the distribution of the virtual machine
- Access is controlled based on control set
- Each recipient should keep the received information for further access to it

Fixed Control Architecture w/ External Repository (FC2)



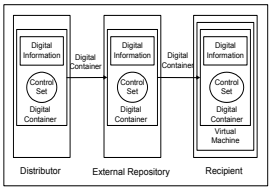
- Similar to FC1, except that digital container is sent to external repository for distribution
- A recipient must connect to the external repository to access or download the digital container
- Accessibility to the content by a single recipient from multiple computers

Embedded Control Architecture w/ Message Push (EC1)



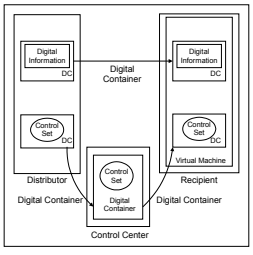
- Control set is embedded in the digital container with digital information
- Distributed content will be controlled based only on the pre-set access rights and usage rules
- After distribution, distributor cannot change the control set of the distributed digital content
- Recipients can access digital content without any network connection
- Only pre-set revocation is available

Embedded Control Architecture w/ External Repository (EC2)



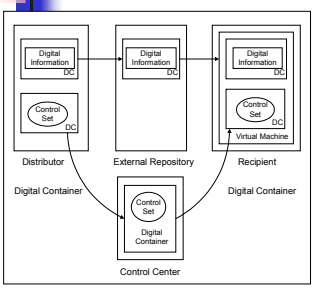
- Digital container is sent to the external repository server for distribution
- If digital container is prohibited from being locally stored, the distributor can revoke a previous granted access by changing control set

External Control Architecture w/ Message Push (XC1)



- Control set can be encapsulated independently from digital content
- Two possible options:
  - Network connection is always required
  - Network connection is required from time to time (one time connection is possible)

External Control Architecture w/ External Repository (XC2)



- Separation of content and access rights
- 4 variations
  - Both encapsulated digital content and encapsulated control set can be stored on recipient's local storage
  - Encapsulated digital content is freely available, but control set cannot be locally stored
  - Only encapsulated control set can be stored
  - Neither can be stored locally

Commercial Solutions

Solution	Organization	NC1	NC2	FC1	FC2	EC1	EC2	XC1	XC2
Adobe Acrobat	Adobe					X			
PDF Merchant & WebBuy	Adobe								X
PageVault	Authentica							X	
SoftSEAL	Breaker Technologies								X
Confidential Courier	Digital Delivery, Inc.					X			
docSPACE	DocSPACE Co.		X						
CIPRESS	Fraunhofer Institute for Computer Graphics & Mitsubishi Co.								X
Cryptolope	IBM							X	
InTether	Infraworks Co.					X			
InterTrust	InterTrust Technologies Co.							X	
RightMarket	RightMarket.com Inc.							X	