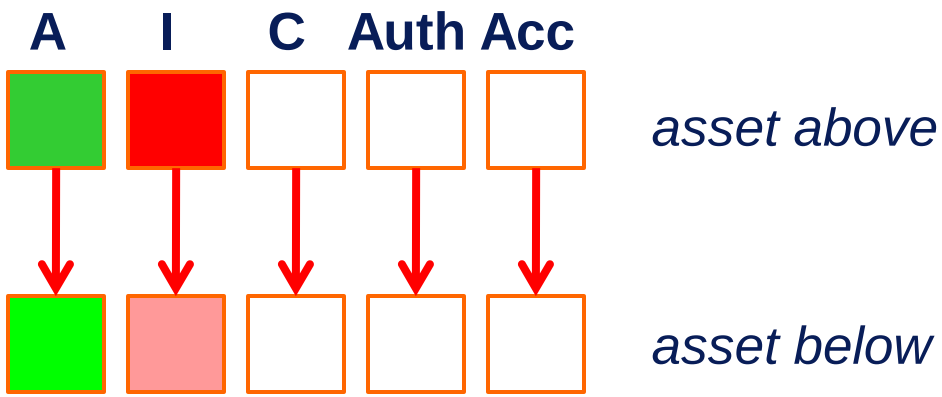
PILAR
Cross-Dimension
Value Propagation

José A. Mañas <jmanas@ar-tools.com>

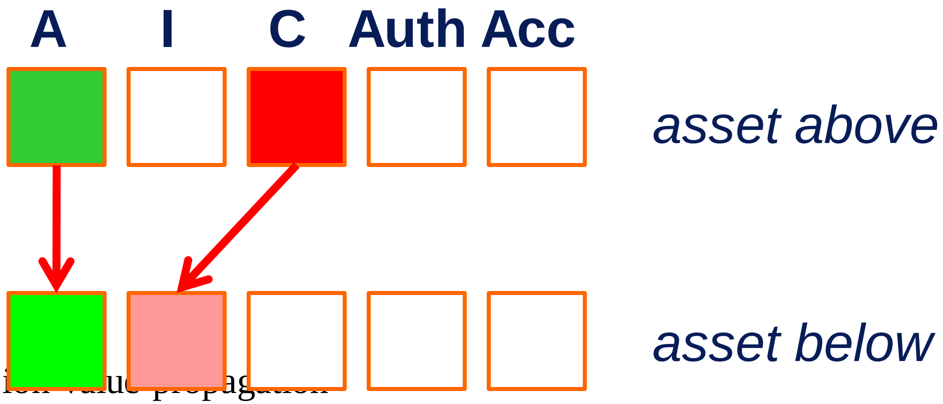
January 25, 2012

dependencies

- Standard is to transfer value within each security dimension

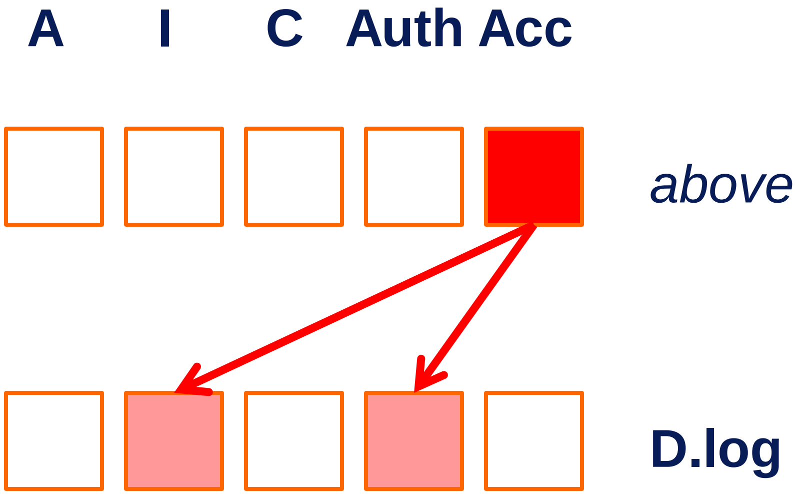


- But sometimes we need to transfer value to another dimension



log

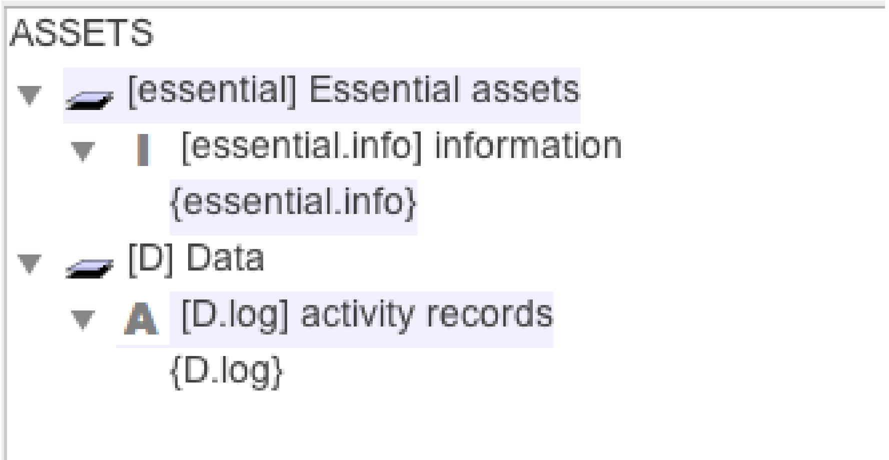
- For instance, accountability requirements imply to protect integrity and authenticity of activity records



- In other words, when the activity record integrity is attacked, the consequences impact the accountability of the system

example

- Assets

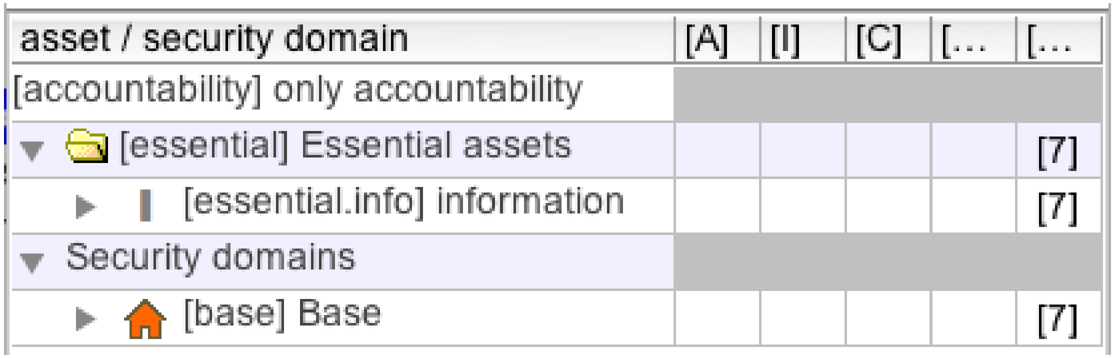


ASSETS

- [essential] Essential assets
  - [essential.info] information
    - {essential.info}
- [D] Data
  - [D.log] activity records
    - {D.log}

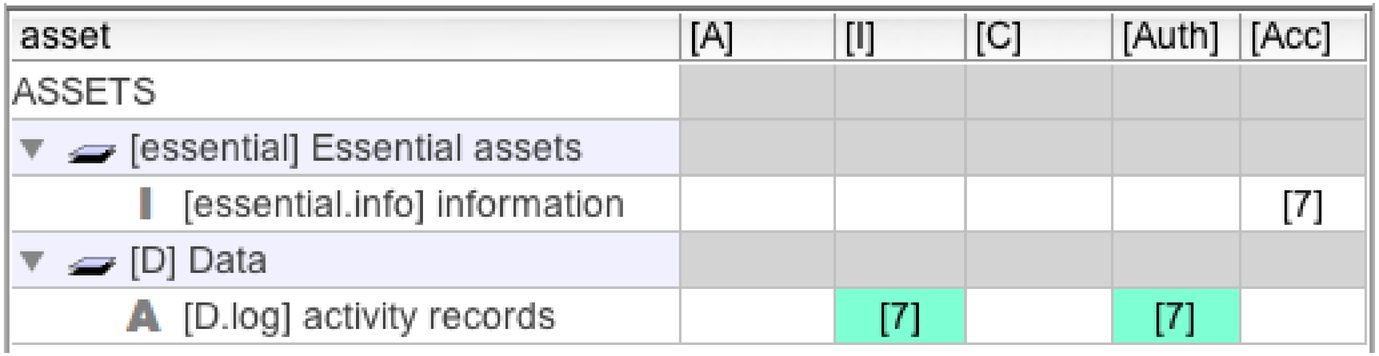
example

- Domain valuation



asset / security domain	[A]	[I]	[C]	[...	[...
[accountability] only accountability					
▼ [essential] Essential assets					[7]
▶ [essential.info] information					[7]
▼ Security domains					
▶ [base] Base					[7]

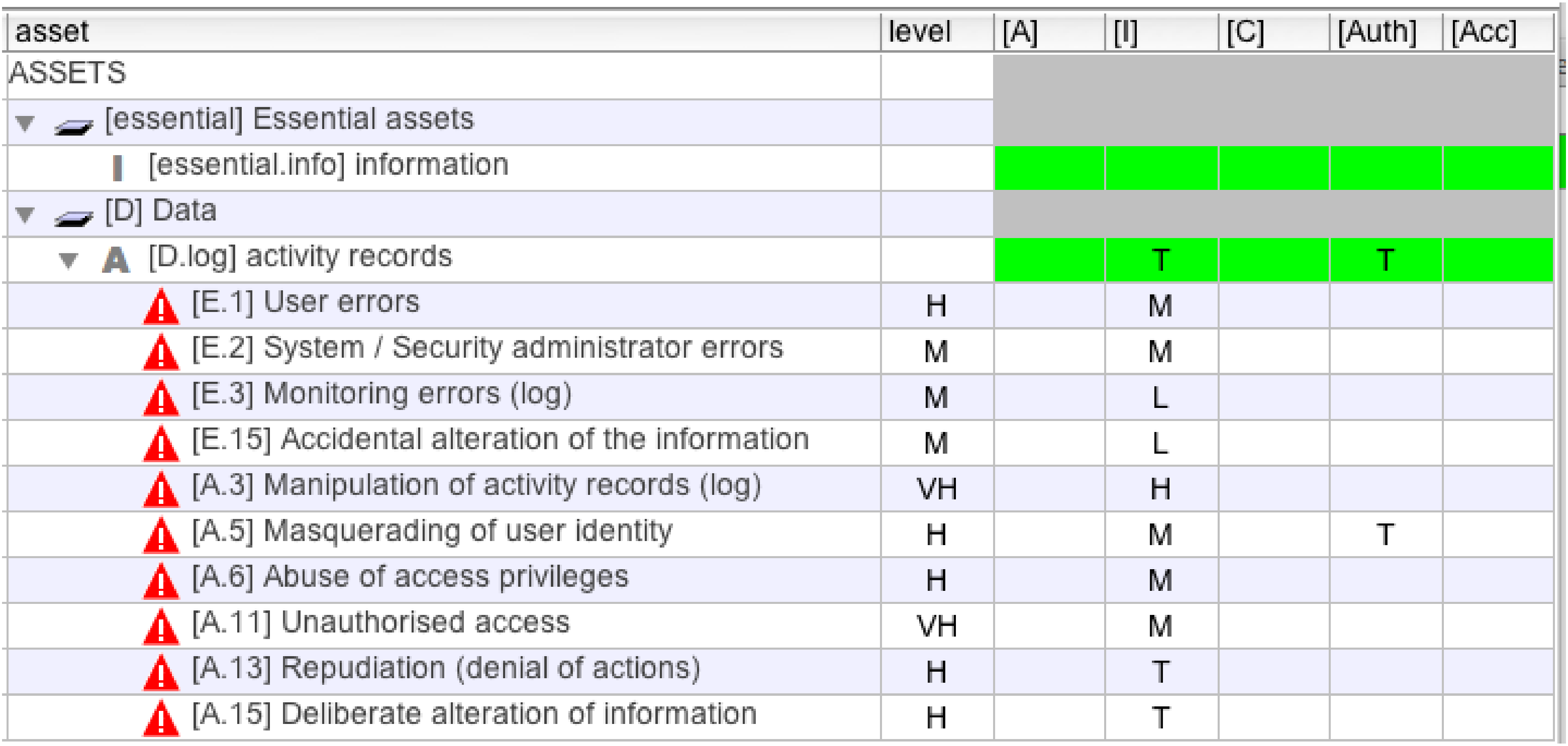
- Asset value: accumulated value



asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS					
▼ [essential] Essential assets					
[essential.info] information					[7]
▼ [D] Data					
A [D.log] activity records		[7]		[7]	

example

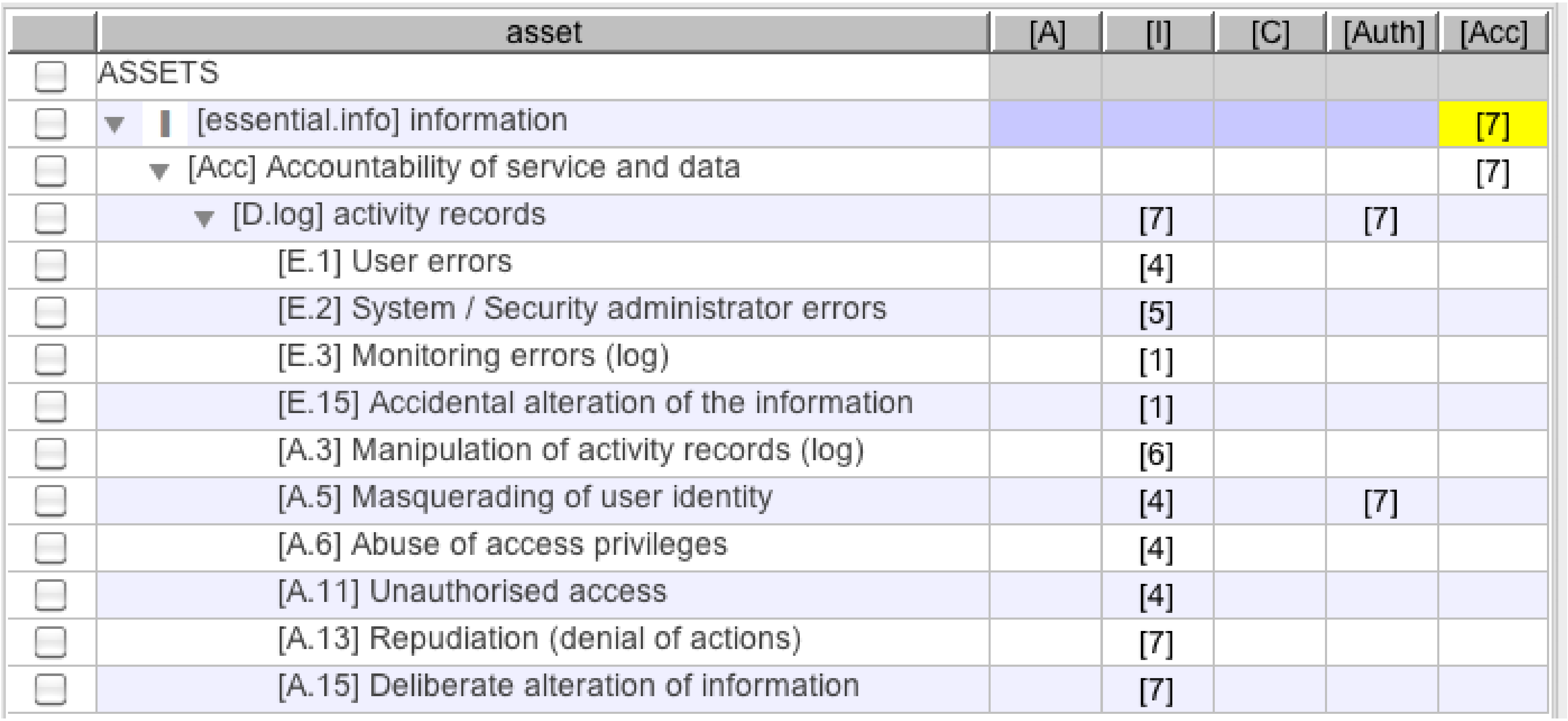
- Threats act on assets below



asset	level	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS						
[essential] Essential assets						
[essential.info] information		🟩	🟩	🟩	🟩	🟩
[D] Data						
[D.log] activity records		🟩	🟩 T	🟩	🟩 T	🟩
⚠ [E.1] User errors	H		M			
⚠ [E.2] System / Security administrator errors	M		M			
⚠ [E.3] Monitoring errors (log)	M		L			
⚠ [E.15] Accidental alteration of the information	M		L			
⚠ [A.3] Manipulation of activity records (log)	VH		H			
⚠ [A.5] Masquerading of user identity	H		M		T	
⚠ [A.6] Abuse of access privileges	H		M			
⚠ [A.11] Unauthorised access	VH		M			
⚠ [A.13] Repudiation (denial of actions)	H		T			
⚠ [A.15] Deliberate alteration of information	H		T			

example

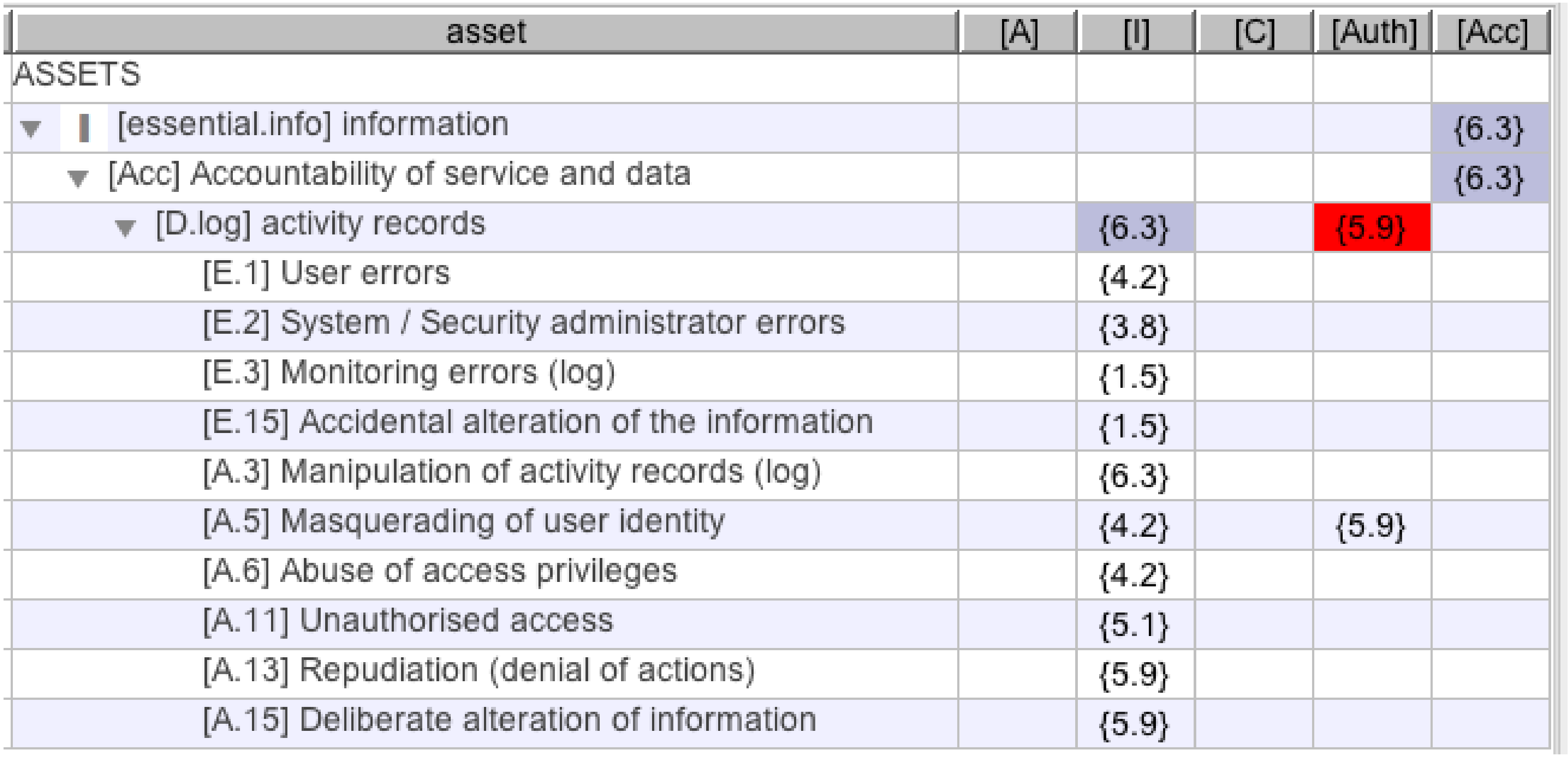
- Impact is deflected on assets above



	asset	[A]	[I]	[C]	[Auth]	[Acc]
□	ASSETS					
□	▼ ▌ [essential.info] information					[7]
□	▼ [Acc] Accountability of service and data					[7]
□	▼ [D.log] activity records		[7]		[7]	
□	[E.1] User errors		[4]			
□	[E.2] System / Security administrator errors		[5]			
□	[E.3] Monitoring errors (log)		[1]			
□	[E.15] Accidental alteration of the information		[1]			
□	[A.3] Manipulation of activity records (log)		[6]			
□	[A.5] Masquerading of user identity		[4]		[7]	
□	[A.6] Abuse of access privileges		[4]			
□	[A.11] Unauthorised access		[4]			
□	[A.13] Repudiation (denial of actions)		[7]			
□	[A.15] Deliberate alteration of information		[7]			

example

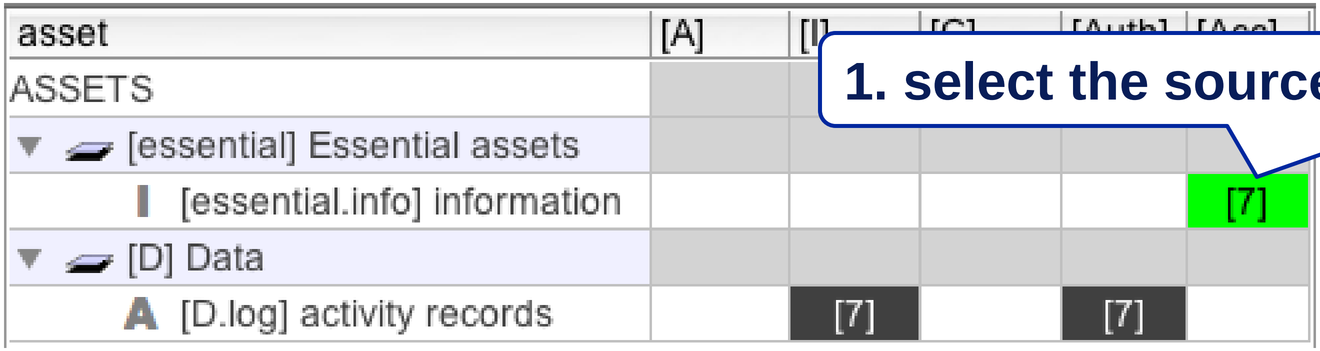
- Risk is deflected on assets above



asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS					
▼ [essential.info] information					{6.3}
▼ [Acc] Accountability of service and data					{6.3}
▼ [D.log] activity records		{6.3}		{5.9}	
[E.1] User errors		{4.2}			
[E.2] System / Security administrator errors		{3.8}			
[E.3] Monitoring errors (log)		{1.5}			
[E.15] Accidental alteration of the information		{1.5}			
[A.3] Manipulation of activity records (log)		{6.3}			
[A.5] Masquerading of user identity		{4.2}		{5.9}	
[A.6] Abuse of access privileges		{4.2}			
[A.11] Unauthorised access		{5.1}			
[A.13] Repudiation (denial of actions)		{5.9}			
[A.15] Deliberate alteration of information		{5.9}			

beyond example

- In a real risk analysis, it may be confusing to discover where is value propagated to
  1. you may use the MARK feature



asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS					
▼ [essential] Essential assets					
[essential.info] information					[7]
▼ [D] Data					
A [D.log] activity records		[7]		[7]	

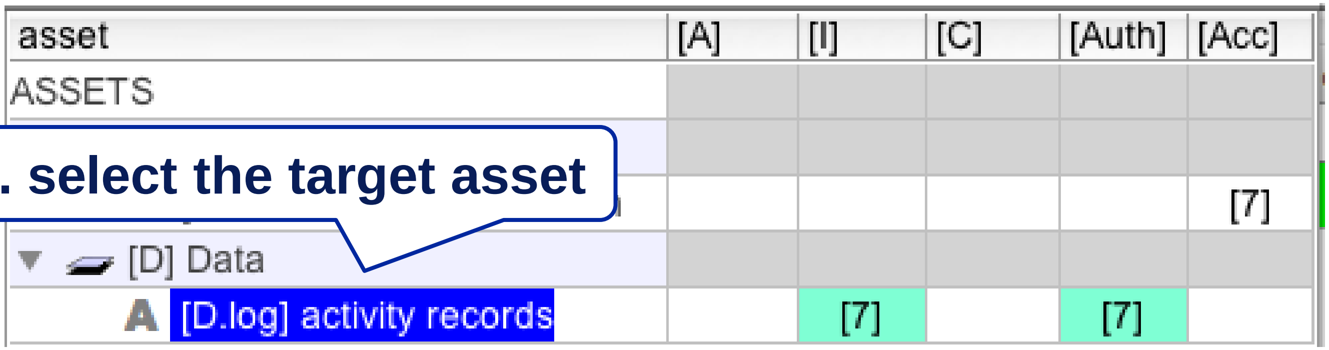
1. select the source value

2. click the button MARK
to see the propagation of the value

beyond example

- In a real risk analysis, it may be confusing to discover where is value propagated to

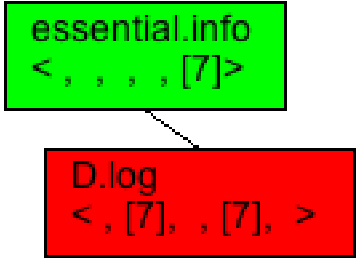
  2. you may use the SOURCES feature



asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS					
					[7]
▼ [D] Data					
A [D.log] activity records		[7]		[7]	

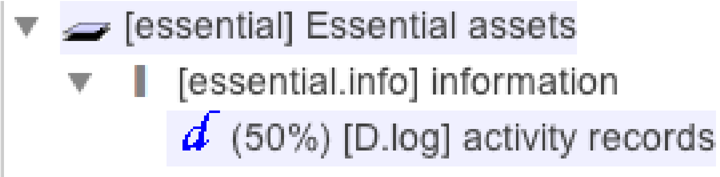
1. select the target asset

2. click the button SOURCES to see the propagation of the value



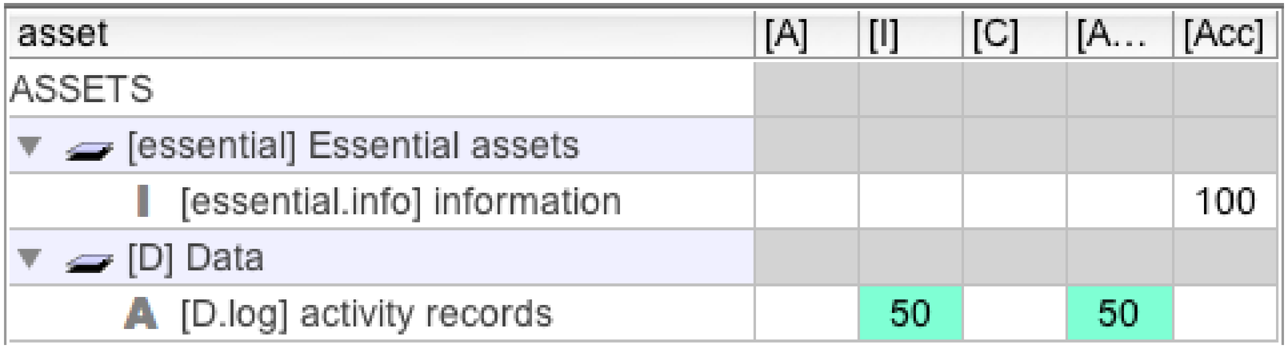
dependency degrees

- If you use both a degree of dependency and a cross-dimension propagation of value



▼ [essential] Essential assets
    ▼ [essential.info] information
        (50%) [D.log] activity records

1. PILAR applies degree of dependency
2. PILAR propagates value

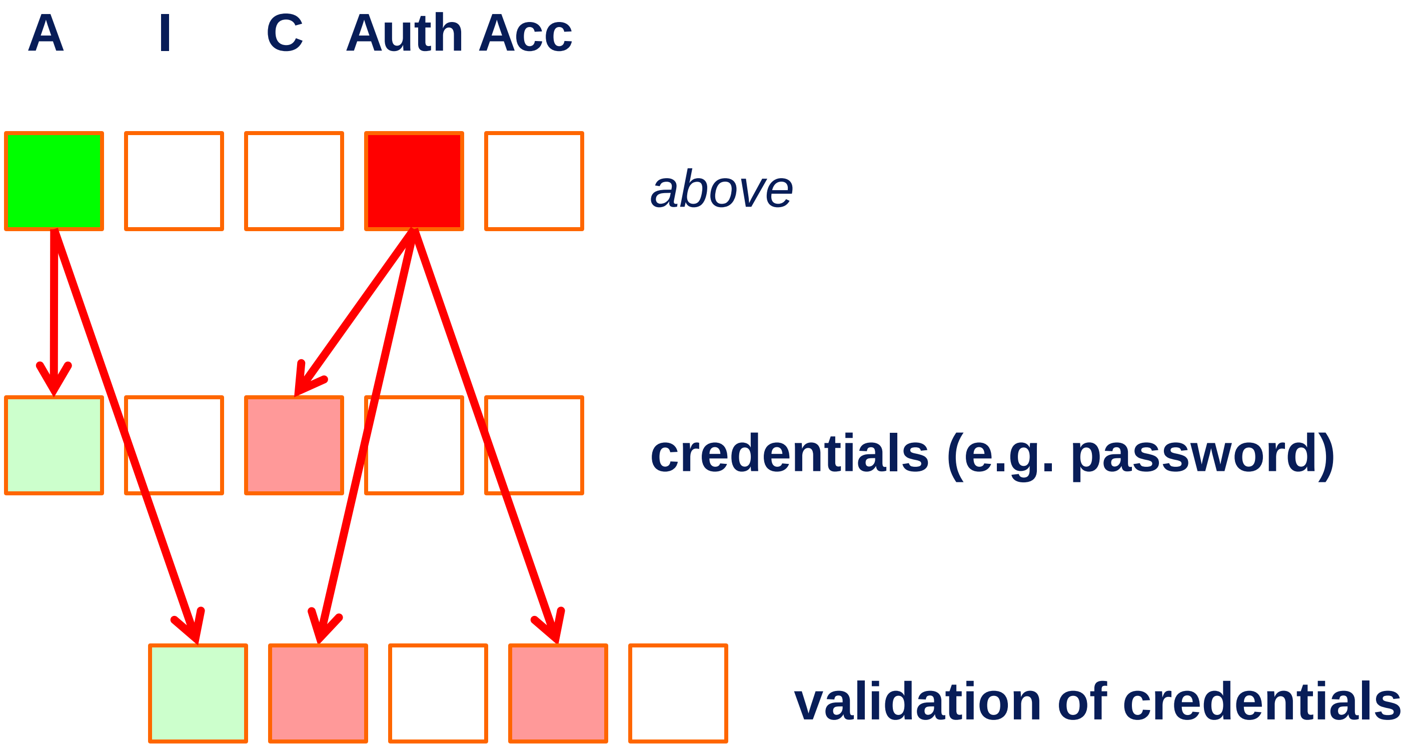


asset	[A]	[I]	[C]	[A…	[Acc]
ASSETS					
▼ [essential] Essential assets					
[essential.info] information					100
▼ [D] Data					
[D.log] activity records		50		50	

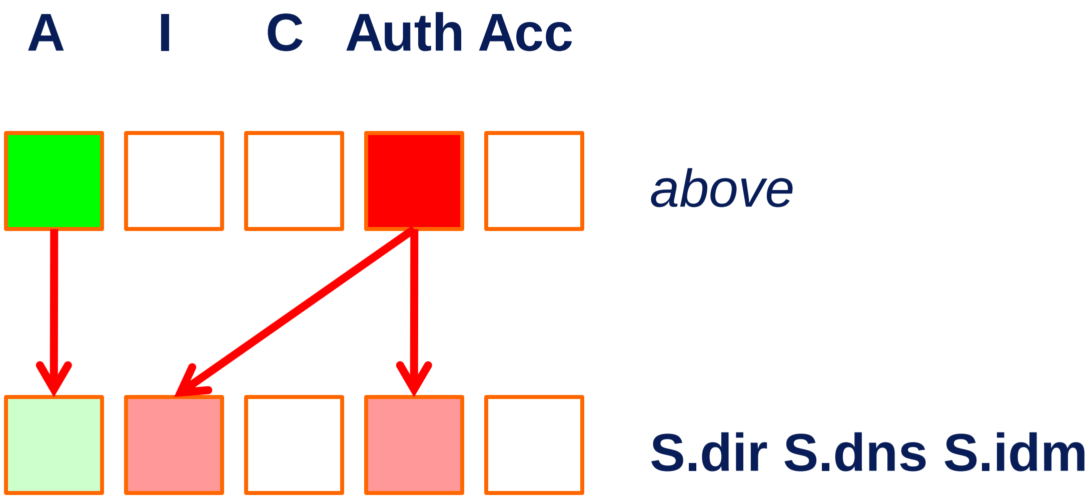
implementation in pilar

- PILAR implements special propagation for
  - D.log: activity records
  - I&A - credentials
  - directory services
  - privilege granting
  - encryption: shared secret & public key
  - signatures: shared secret & public key
  - vpn: virtual private networks
- The behaviour is hardcoded, and it is driven by the class of the asset below
  - if you need to skip this feature, avoid those standard classes

identification & authentication



directory



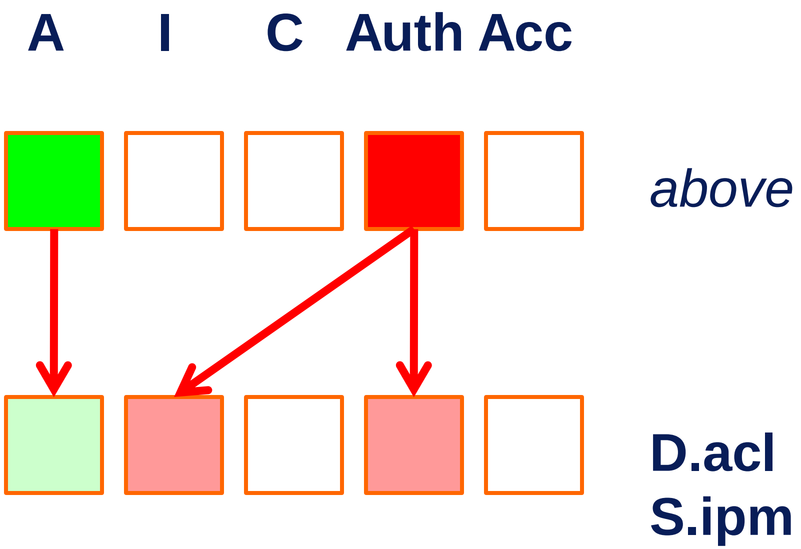
A I C Auth Acc

above

S.dir S.dns S.idm

cross-dimension value propagation

privilege granting

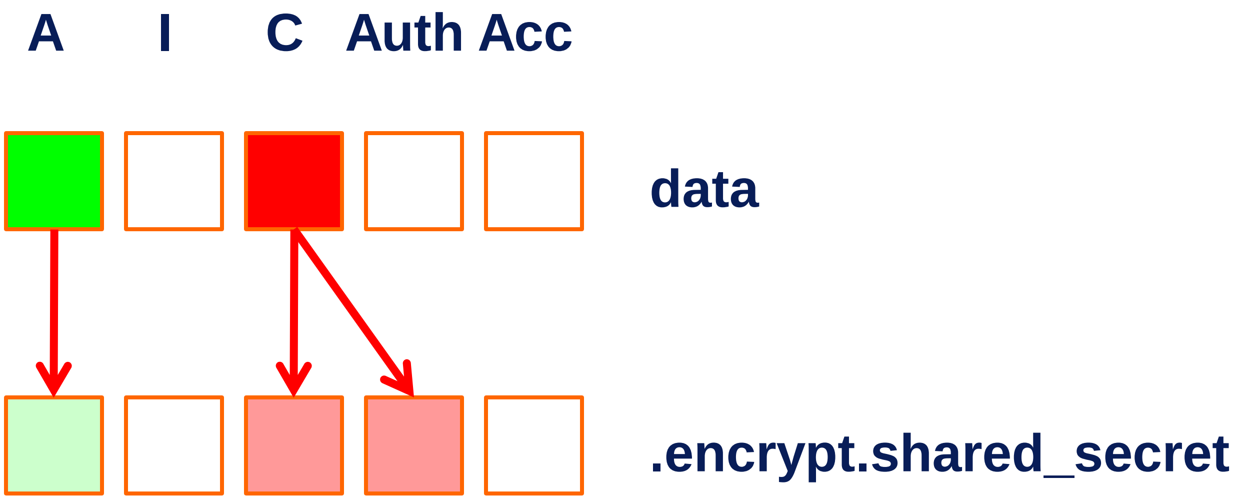


A I C Auth Acc

above

D.acl
S.ipm

encryption

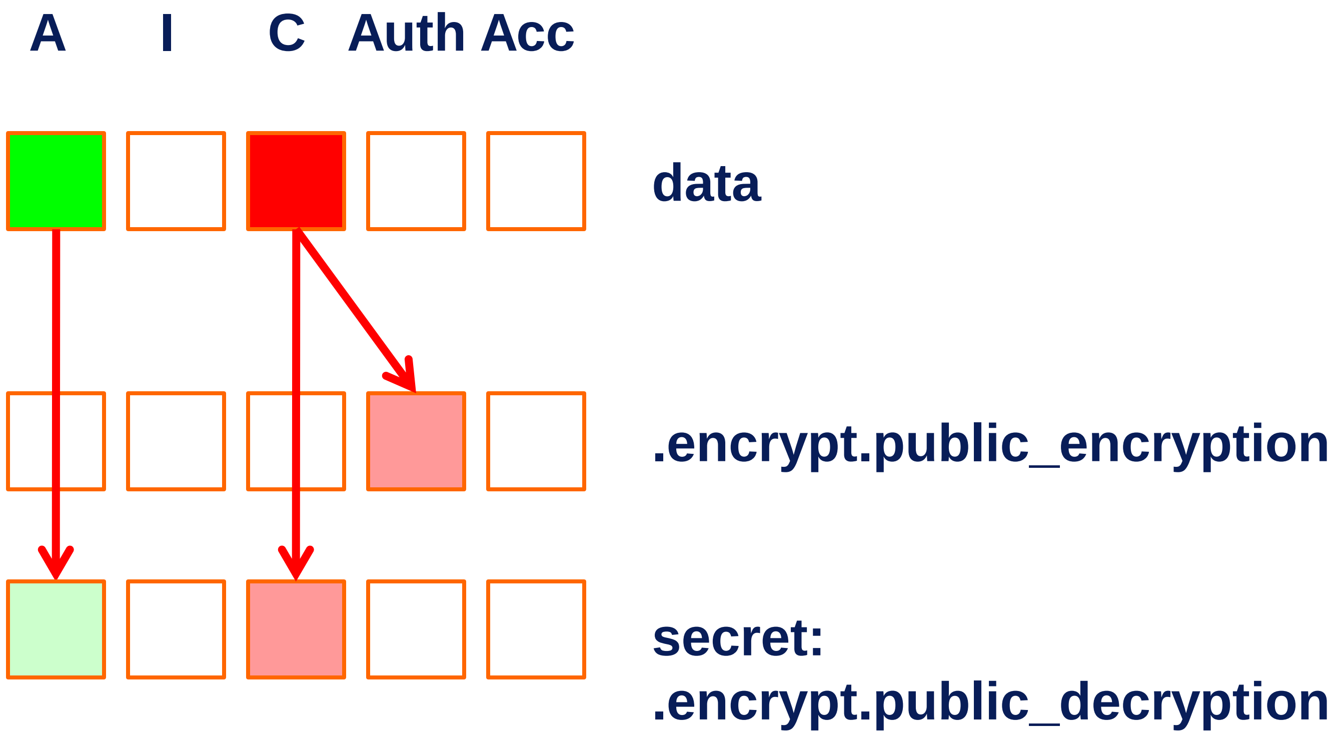


A I C Auth Acc

data

.encrypt.shared_secret

encryption



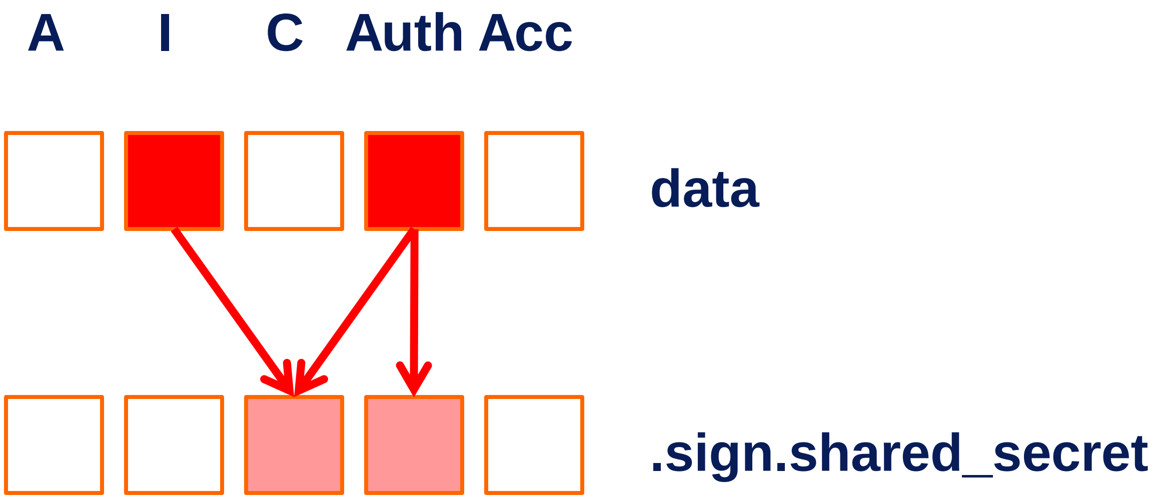
A I C Auth Acc

data

.encrypt.public_encryption

secret:
.encrypt.public_decryption

signature

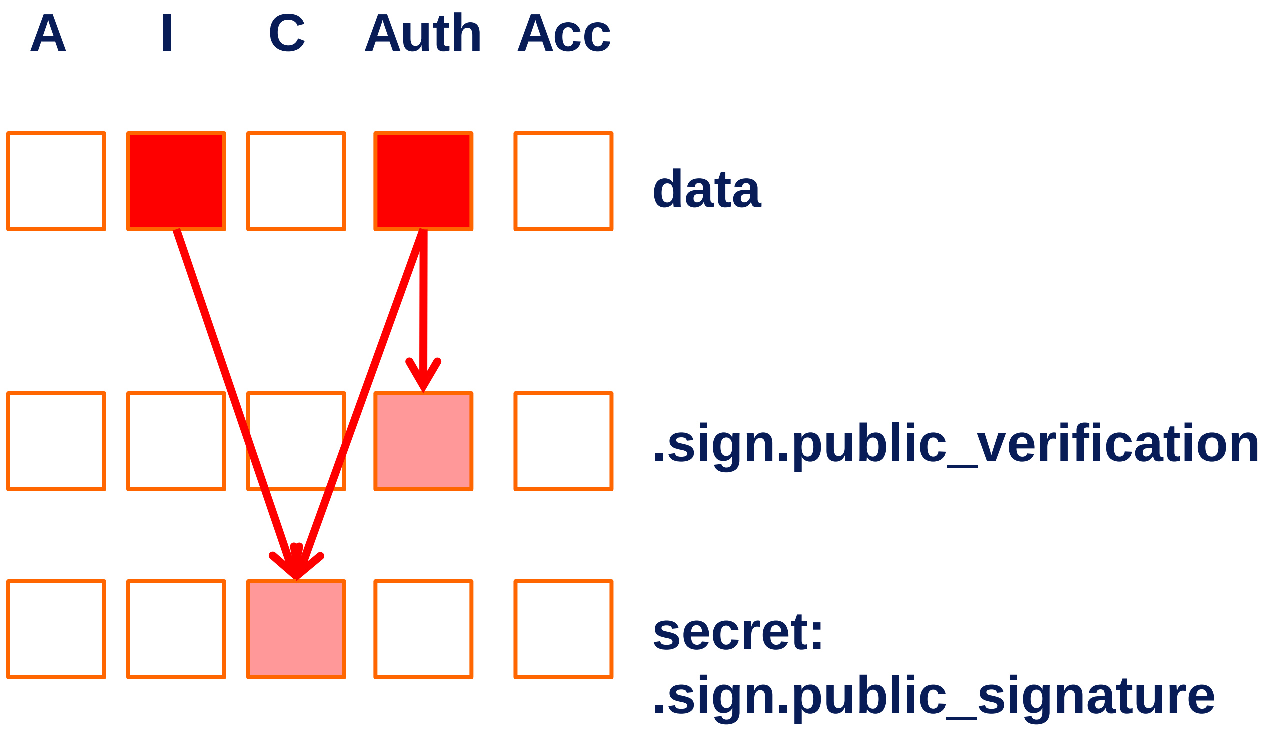


A I C Auth Acc

data

.sign.shared_secret

signature



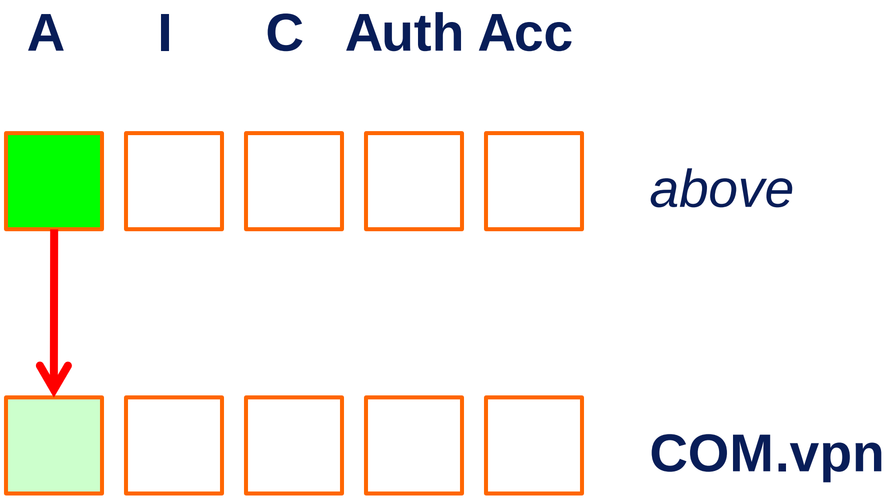
A I C Auth Acc

data

.sign.public_verification

secret:
.sign.public_signature

vpn



A I C Auth Acc

above

COM.vpn