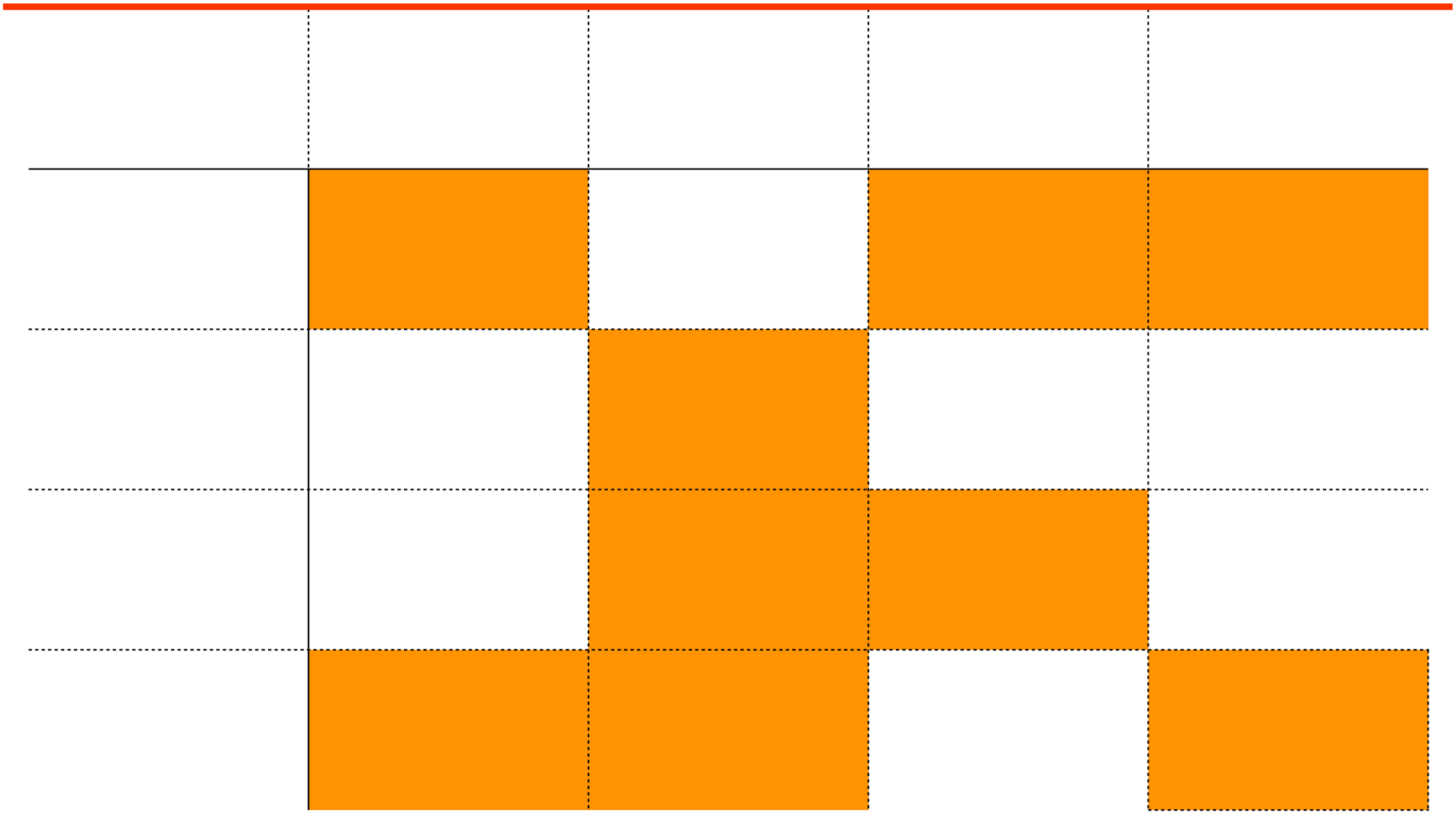
Verify what?

Navigating the Attack Surface

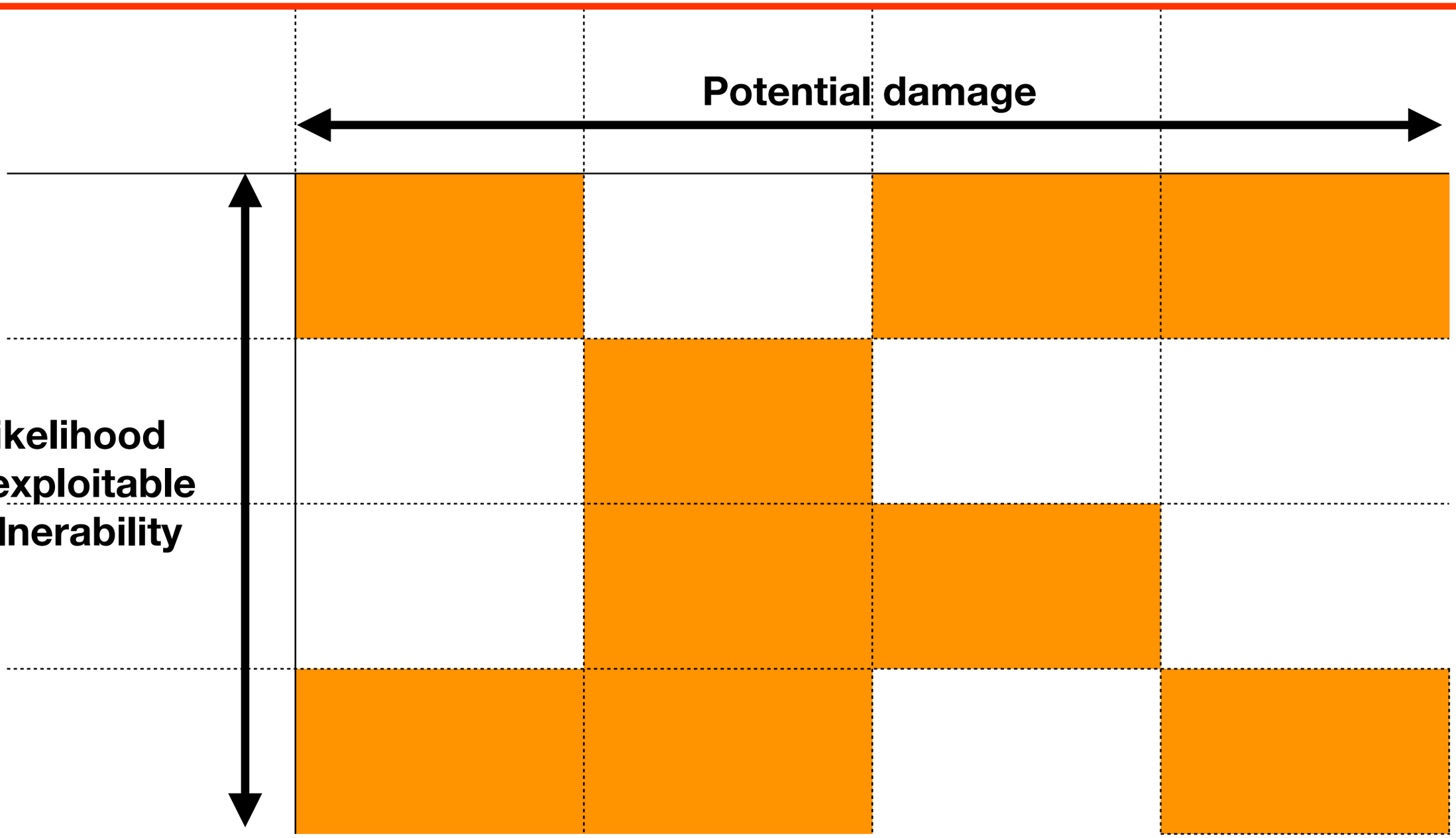
Mark S. Miller, Google

Formal Methods meets JavaScript
Imperial College, March 2018

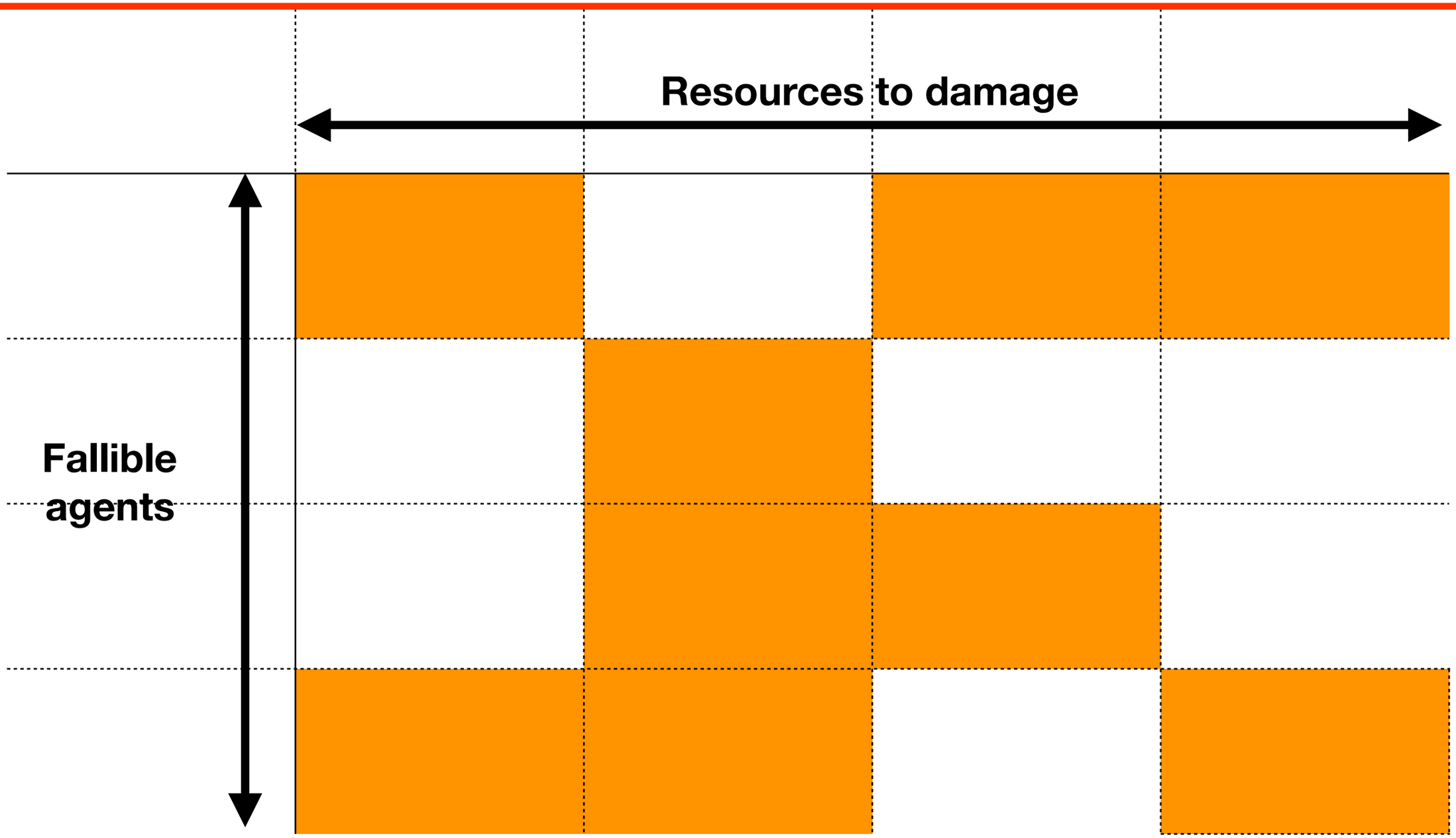
Risk as Attack Surface



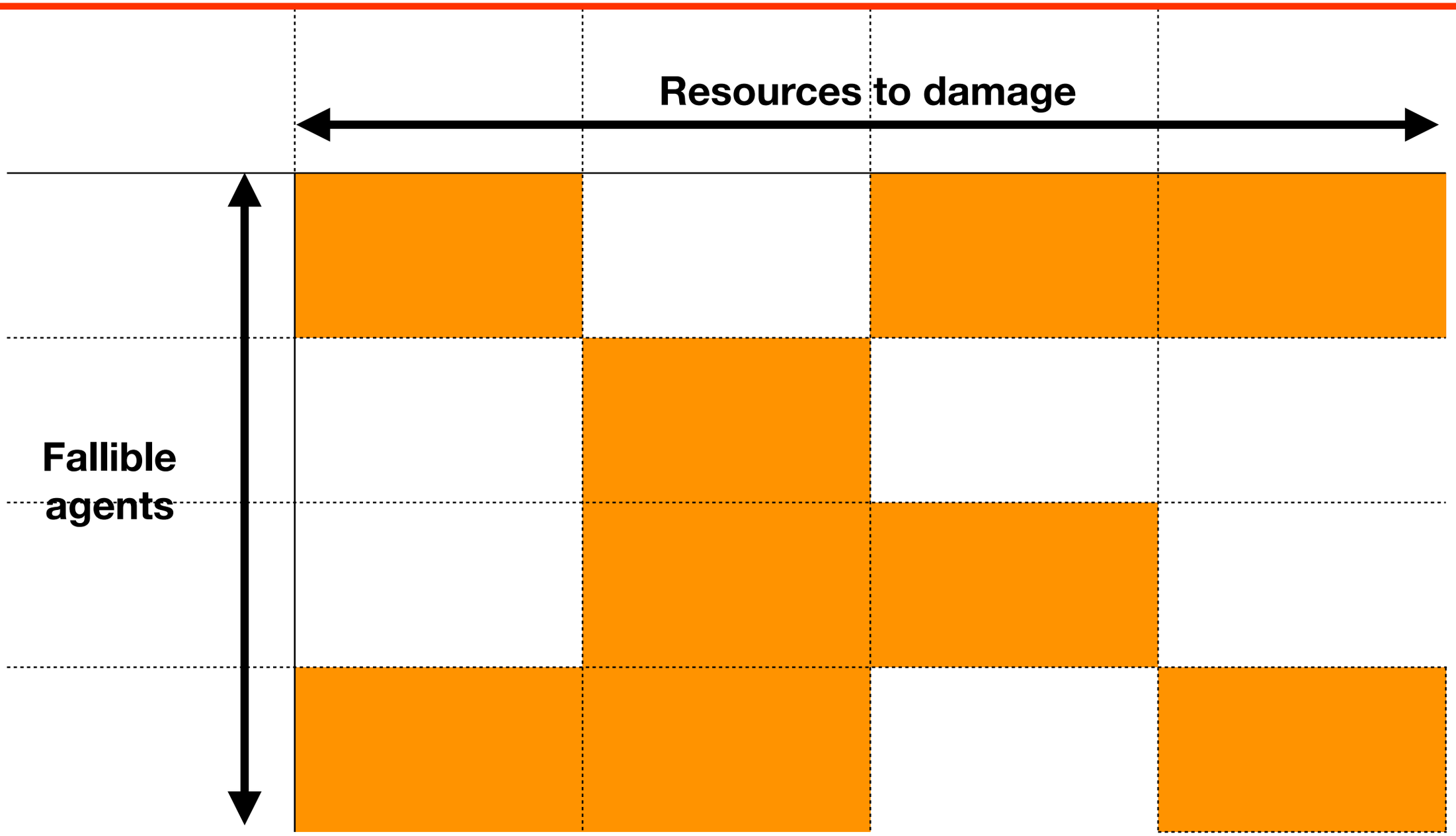
Expected Risk: $\int$ likelihood * damage



Expected Risk: $\int$ likelihood * damage



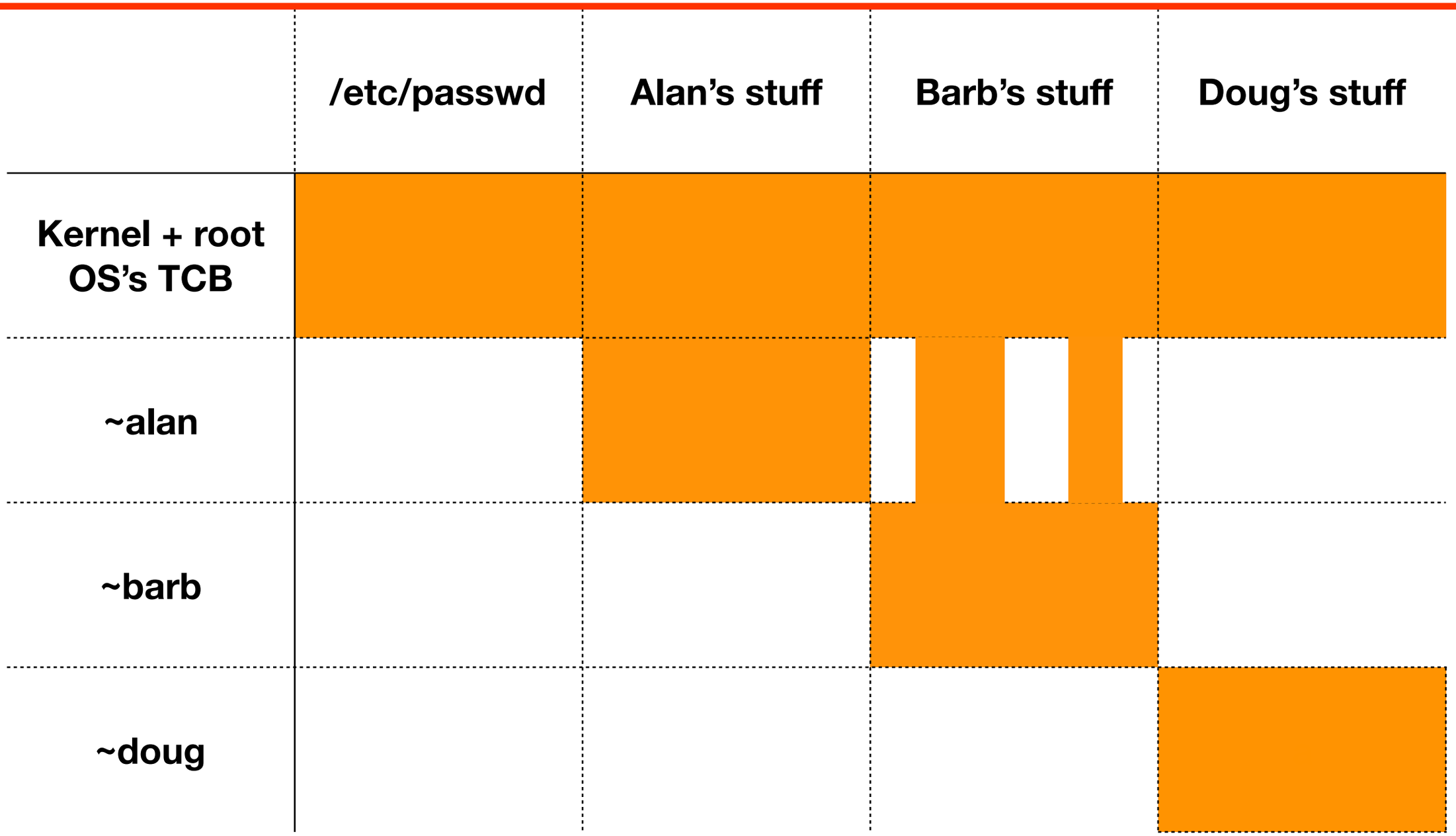
Access Matrix
Permission or Authority?

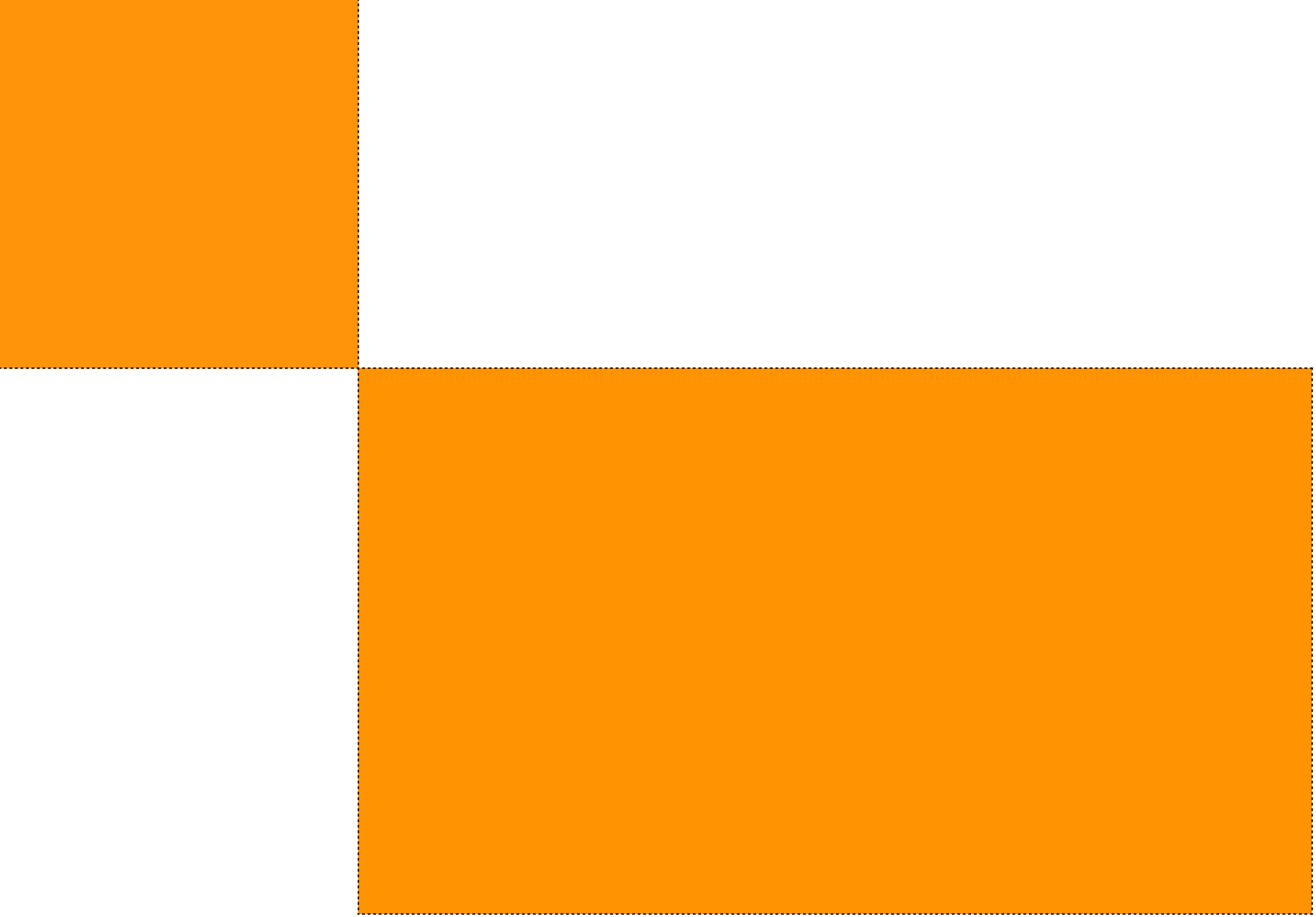


Hollow Out the Attack Surface!

	/etc/passwd	Alan's stuff	Barb's stuff	Doug's stuff
Kernel + root OS's TCB				
~alan				
~barb				
~doug				

Decouple accounts





Decouple applications

	contact info	pgp keyring	calc.xls	Net access
Shell, Desktop				
Browser				
Spreadsheet				
Email client				

Decouple apps

	contact info	pgp keyring	calc.xls	Net access
MobileOS Doug's TCB				
Browser app				
Spreadsheet doc				
Mail app				

Decouple apps

	contact info	pgp keyring	calc.xls	Net access
MobileOS Doug's TCB	■	■	■	■
Browser app			■	■
Spreadsheet doc			■	
Mail app	■	■		■

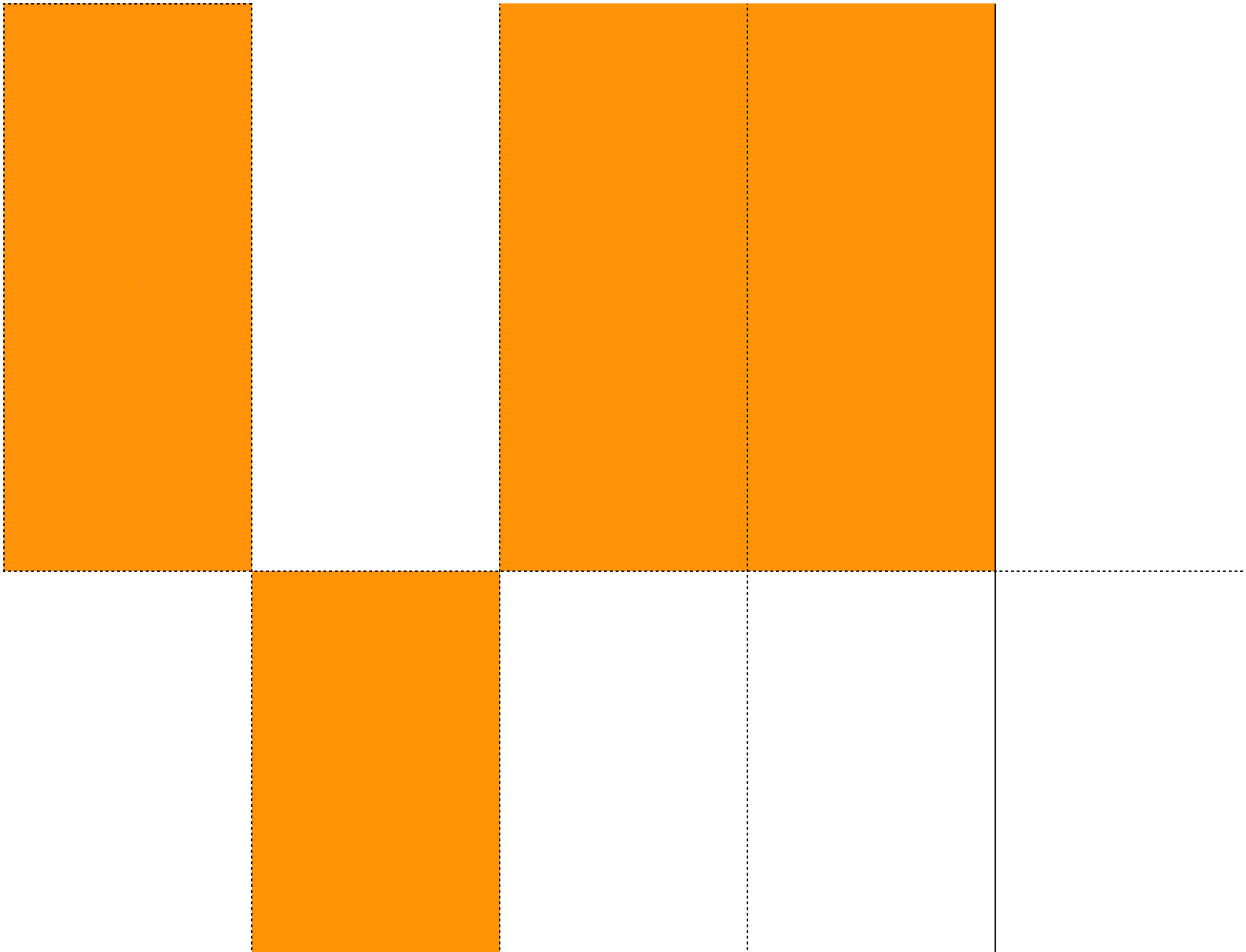
Substrate	Historical System	System
Hardware	CMNM, Plessey 250, C.mmp, CM*, CAP, Flex, IBM System/38, Intel 432	Crash-SAFE, CHERI, Risc-V
OS	DVH, Hydra, StarOS, RATS, Cal-TSS, PSOS, NLTSS, Spring	Capsicum, CloudABI, Genode, Barrelfish, Fuchsia
KeyKOS family OS	Gnosis, KeyKOS, GuardOS, EROS, CapROS, Coyotos	seL4
Distributed OS	Ameoba, Mach, Midori	
Language	Gedanken, W7, J-Kernel, Joe-E, Emily, CaPerl, Caja, Tamed Pict, Plash	Monte, Frozen Realms, shill, Wyvern, wasm-gc
Distributed Language	Act-1, Eden, Emerald, Vulcan, Joule, E, Oz-E, M#	Pony, Kappa, Dr.SES
Distributed Storage	Scoopfs	Tahoe-LAFS
Crypto Protocol	DCCS, CapTP, Foolscap, Client Utility, Waterken	COAST, Cap'n Proto
Offline Certs	SPKI/SDSI, E-Speak, CapCert	Macaroons, Id-ocap
Blockchain		Gravity, Dfinity, RChain, Cosmos, Veres One, Sovrin, Agoric Systems
User Interface	CapDesk, Scoopfs, Belay	Sandstorm

Substrate	Historical System	System
Hardware	CMNM, Plessey 250, C.mmp, CM*, CAP, Flex, IBM System/38, Intel 432	Crash-SAFE, CHERI, Risc-V
OS	DVH, Hydra, StarOS, RATS, Cal-TSS, PSOS, NLTSS, Spring	Capsicum, CloudABI, Genode, Barrelfish, Fuchsia
KeyKOS family OS	Gnosis, KeyKOS, GuardOS, EROS, CapROS, Coyotos	seL4
Distributed OS	Ameoba, Mach, Midori	
Language	Gedanken, W7, J-Kernel, Joe-E, Emily, CaPerl, **Caja**, Tamed Pict, Plash	Monte, **Frozen Realms**, shill, Wyvern, **wasm-gc**
Distributed Language	Act-1, Eden, Emerald, Vulcan, Joule, E, Oz-E, M#	Pony, Kappa, **Dr.SES**
Distributed Storage	Scoopfs	Tahoe-LAFS
Crypto Protocol	DCCS, CapTP, Foolscap, Client Utility, **Waterken**	COAST, Cap'n Proto
Offline Certs	SPKI/SDSI, E-Speak, CapCert	Macaroons, Id-ocap
Blockchain		**Gravity**, **Dfinity**, RChain, Cosmos, Veres One, Sovrin, **Agoric Systems**
User Interface	CapDesk, Scoopfs, **Belay**	Sandstorm

Substrate	Historical System	System
Hardware	CMNM, Plessey 250, C.mmp, CM*, CAP, Flex, IBM System/38, Intel 432	Crash-SAFE, CHERI, Risc-V
OS	DVH, Hydra, StarOS, RATS, Cal-TSS, PSOS, NLTSS, Spring	Capsicum, CloudABI, Genode, Barrelfish, Fuchsia
KeyKOS family OS	Gnosis, KeyKOS, GuardOS, EROS, CapROS, Coyotos	seL4
Distributed OS	Ameoba, Mach, Midori	
Language	Gedanken, W7, J-Kernel, Joe-E, Emily, CaPerl, Caja, Tamed Pict, Plash	Monte, Frozen Realms, shill, Wyvern, wasm-gc
Distributed Language	Act-1, Eden, Emerald, Vulcan, Joule, **E**, Oz-E, M#	Pony, Kappa, Dr.SES
Distributed Storage	Scoopfs	Tahoe-LAFS
Crypto Protocol	DCCS, **CapTP**, Foolscap, Client Utility, Waterken	COAST, Cap'n Proto
Offline Certs	SPKI/SDSI, E-Speak, CapCert	Macaroons, ld-ocap
Blockchain		Gravity, Dfinity, RChain, Cosmos, Veres One, Sovrin, Agoric Systems
User Interface	**CapDesk**, Scoopfs, Belay	Sandstorm

Decouple caplets

	contact info	pgp keyring	calc.xls	Net access
E, CapDesk Doug's TCB	■	■	■	■
DarpaBrowser caplet				■
Excel in Polaris			■	
CapMail caplet	■	■		■



Decouple modules

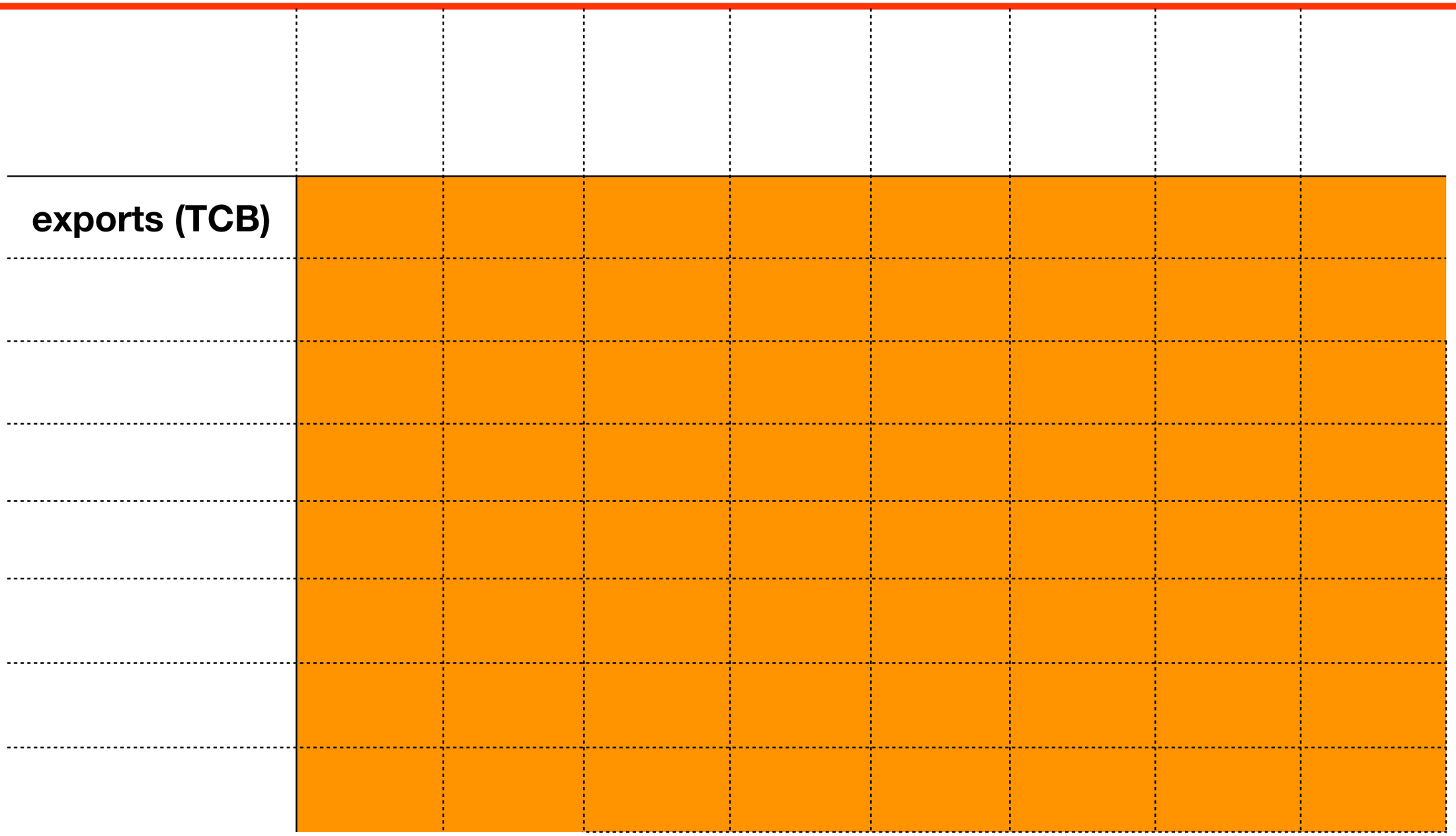
	contact info	pgp keyring	calc.xls	Net access
main() CapMail's TCB	■	■		■
address book	■	■		■
gpg plugin	■	■		■
SMTP, POP stacks	■	■		■

Decouple modules

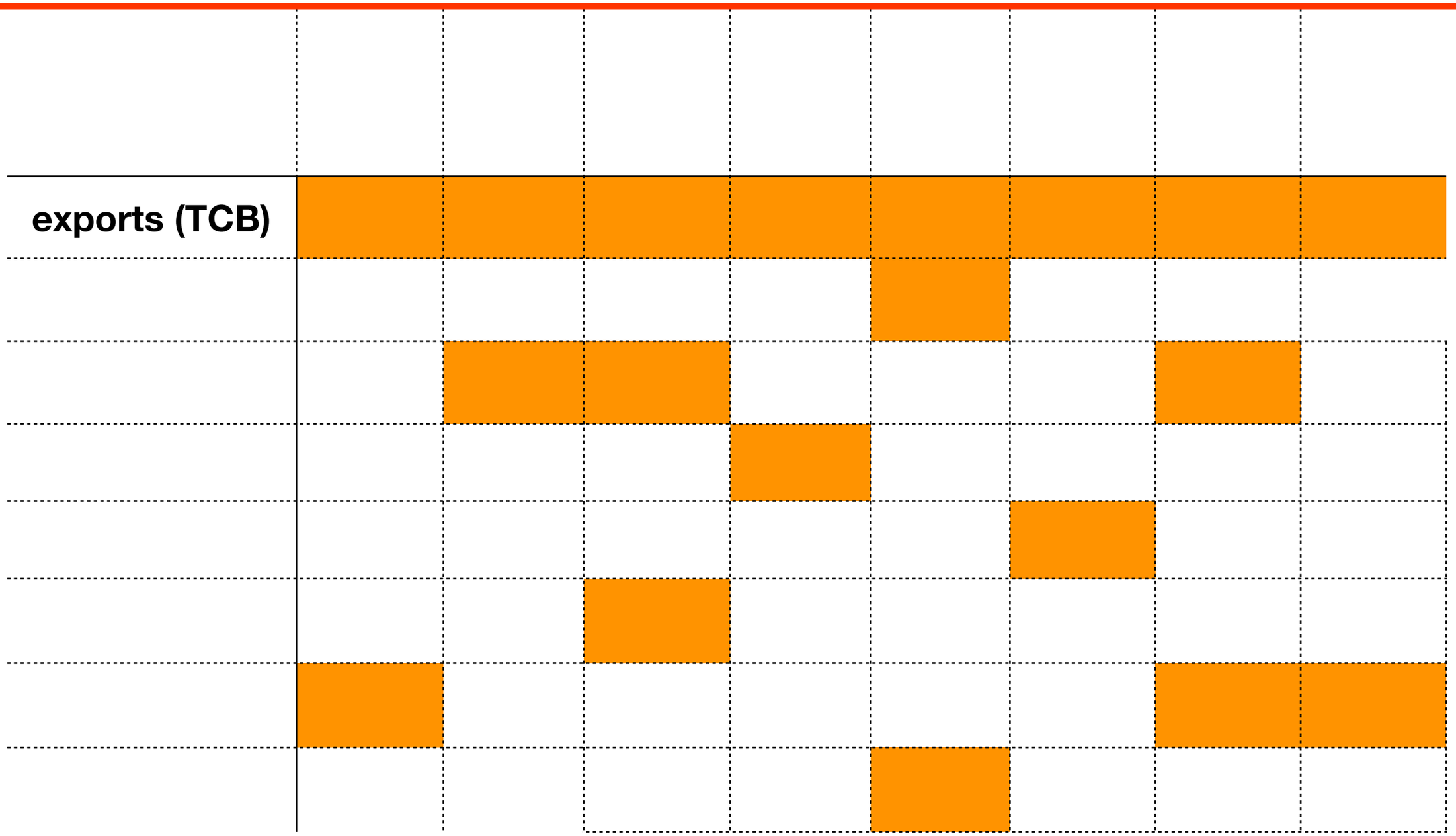
	contact info	pgp keyring	calc.xls	Net access
main() CapMail's TCB	■	■		■
address book	■			
gpg plugin	■	■		
SMTP, POP stacks				■

n

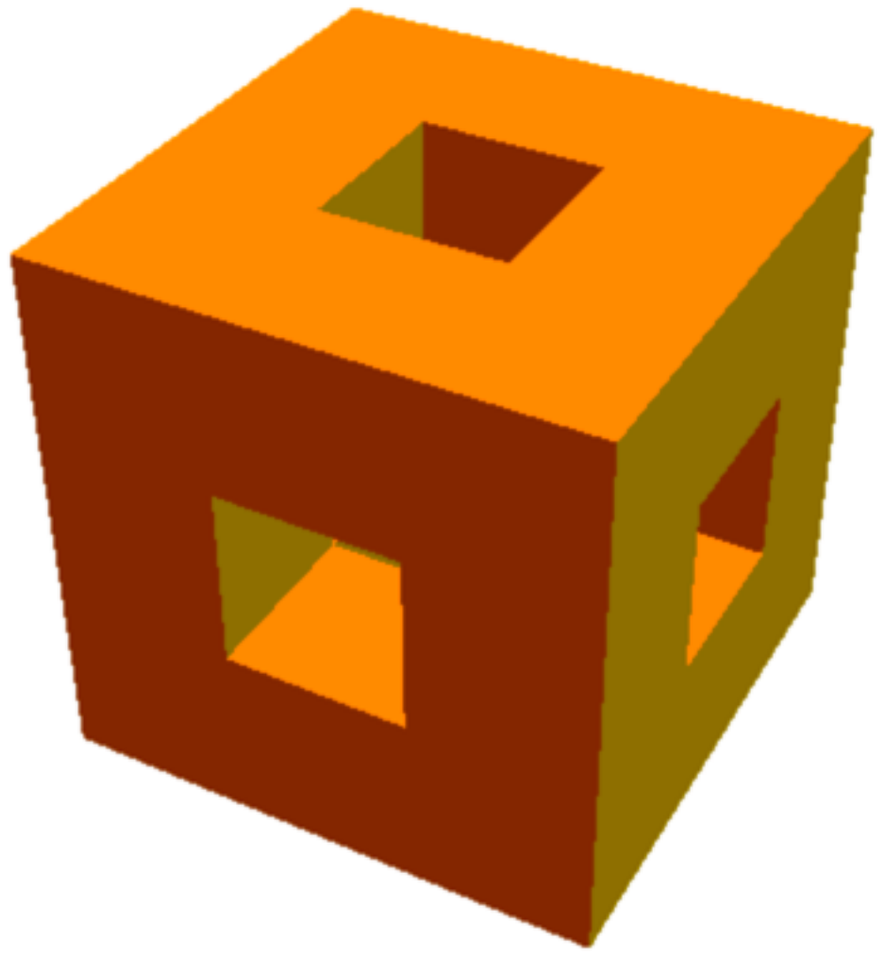
Decouple objects



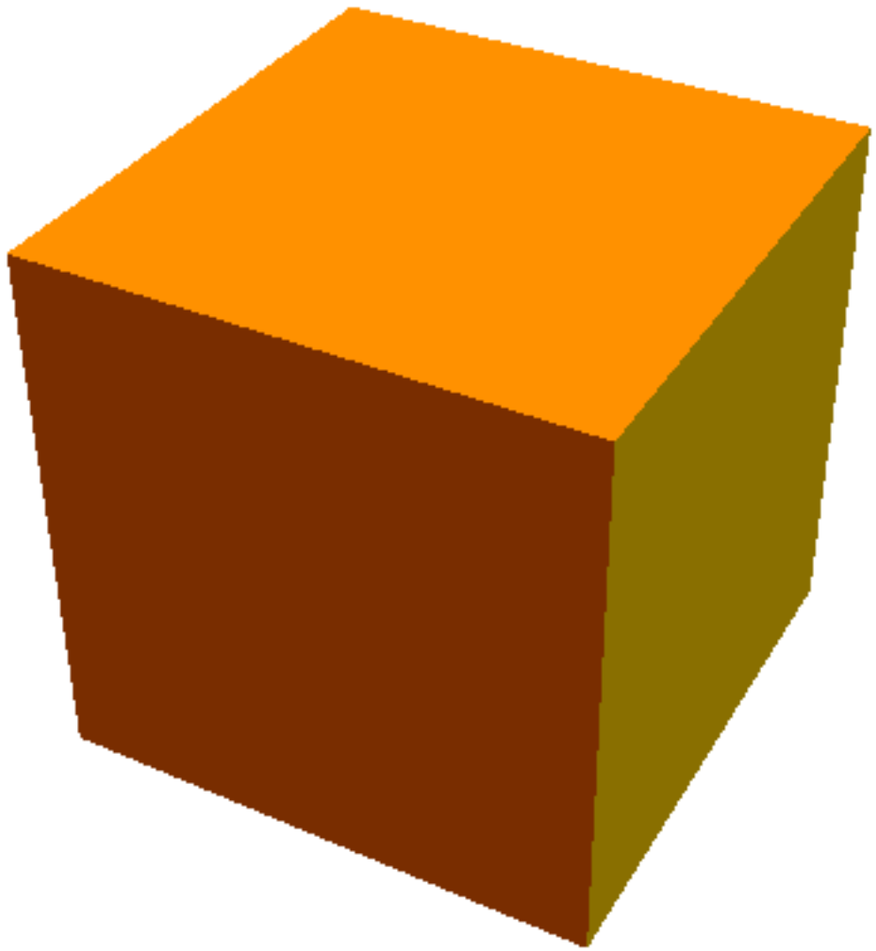
Decouple objects



Defensive Programming



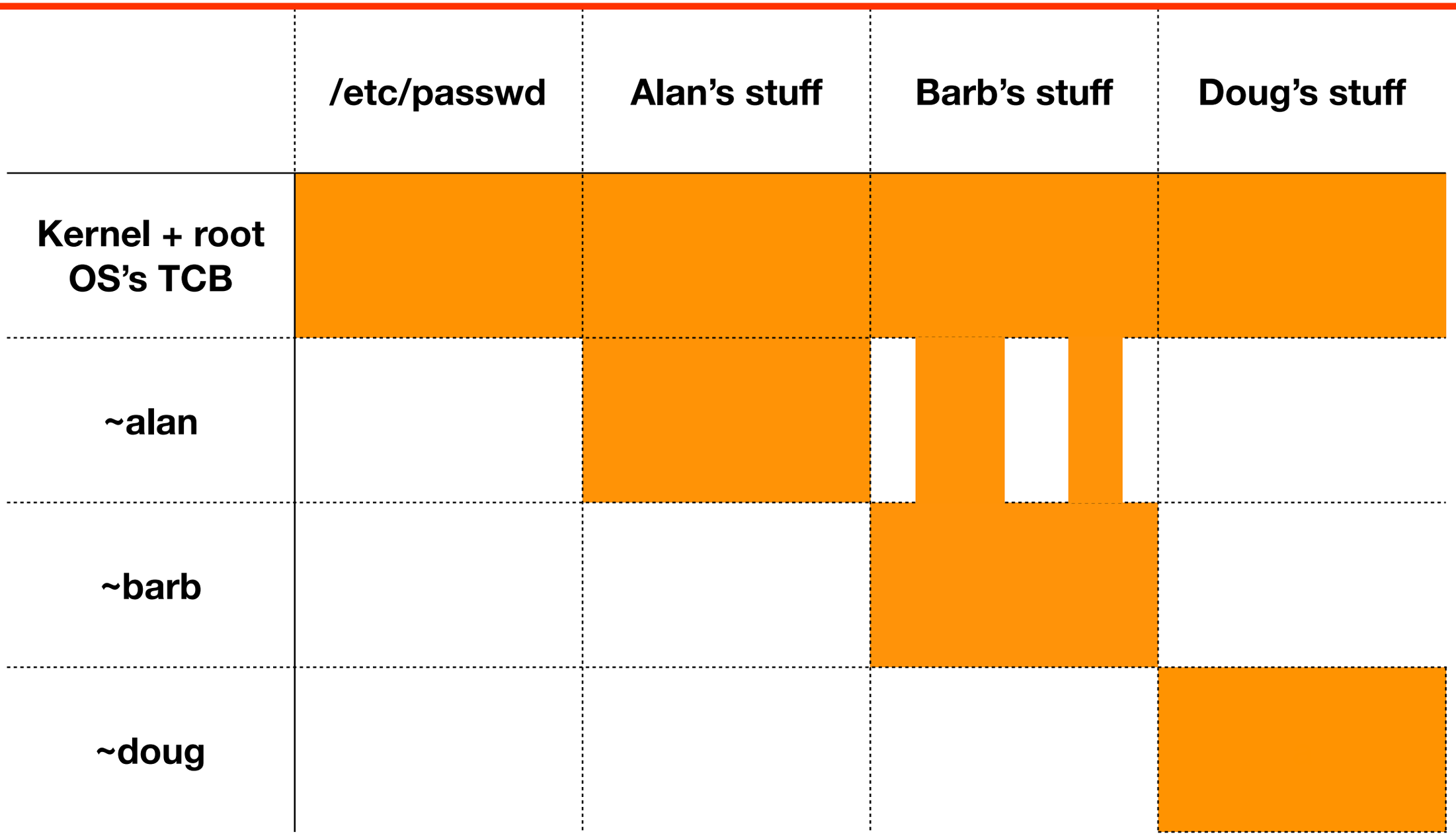
Defense in Depth



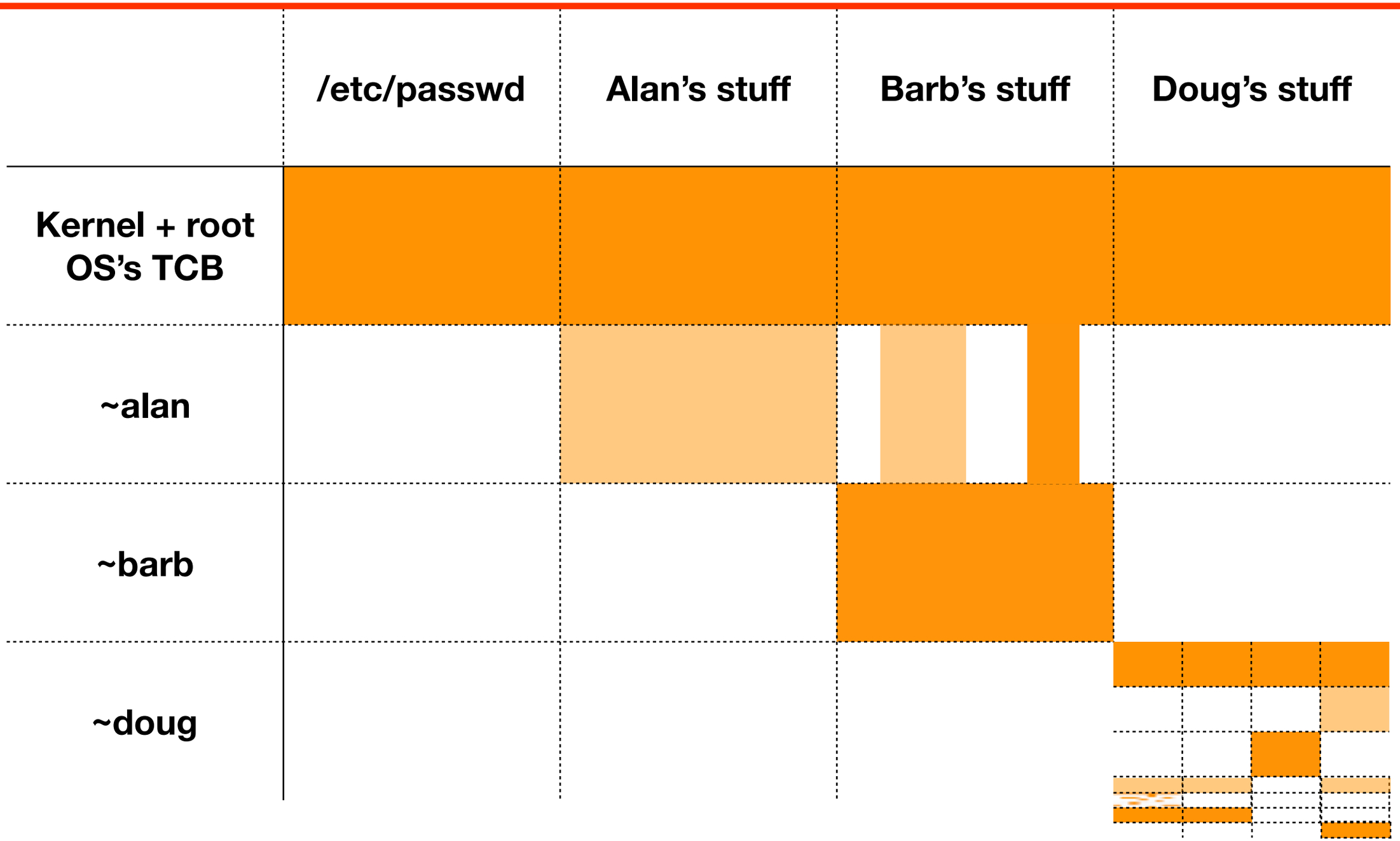
Reduce area
Mix of strategies

	/etc/passwd	Alan's stuff	Barb's stuff	Doug's stuff
Kernel + root OS's TCB				
~alan				
~barb				
~doug				

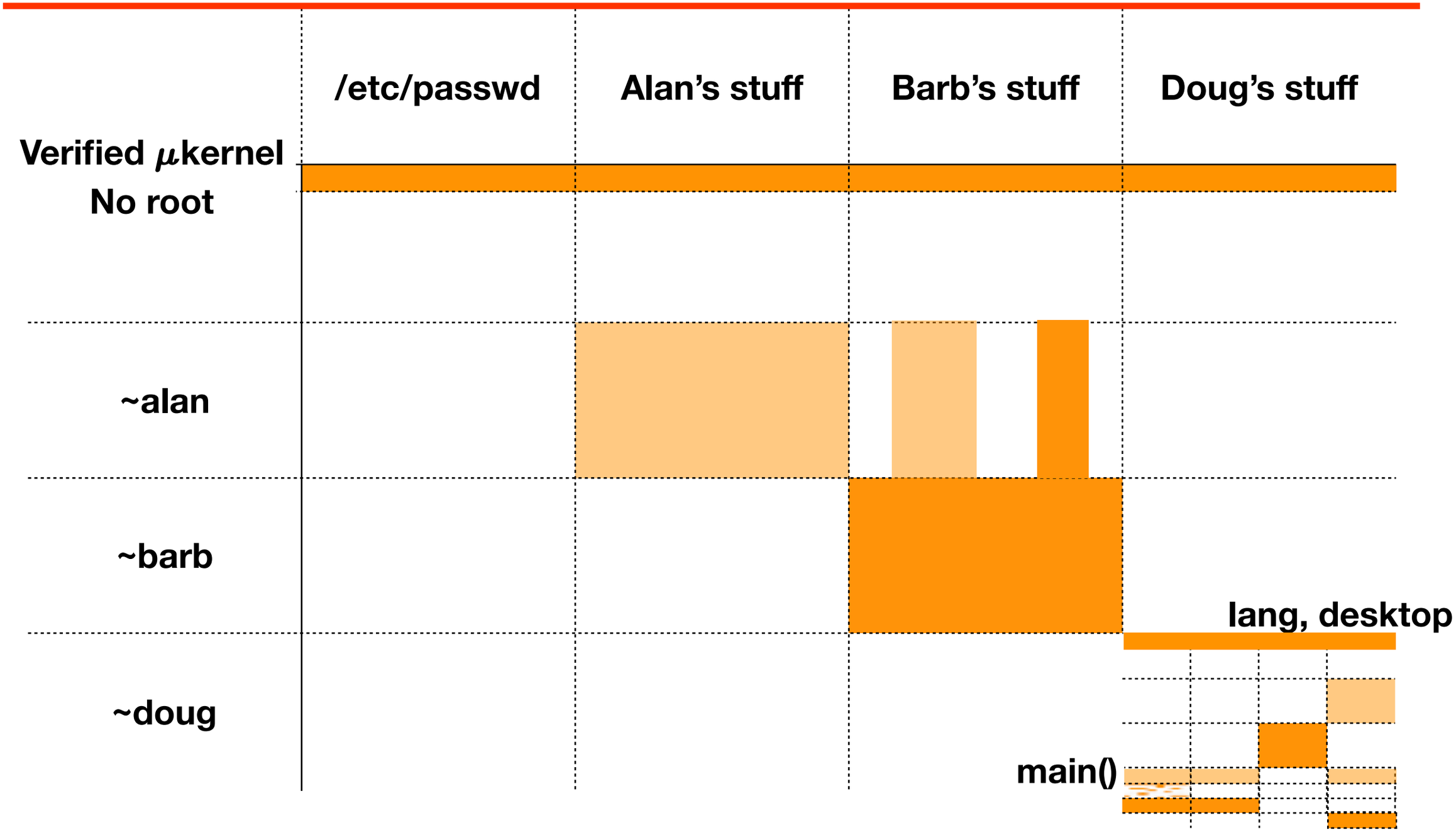
Reduce horizontal space
POLA — Principle of Least Authority



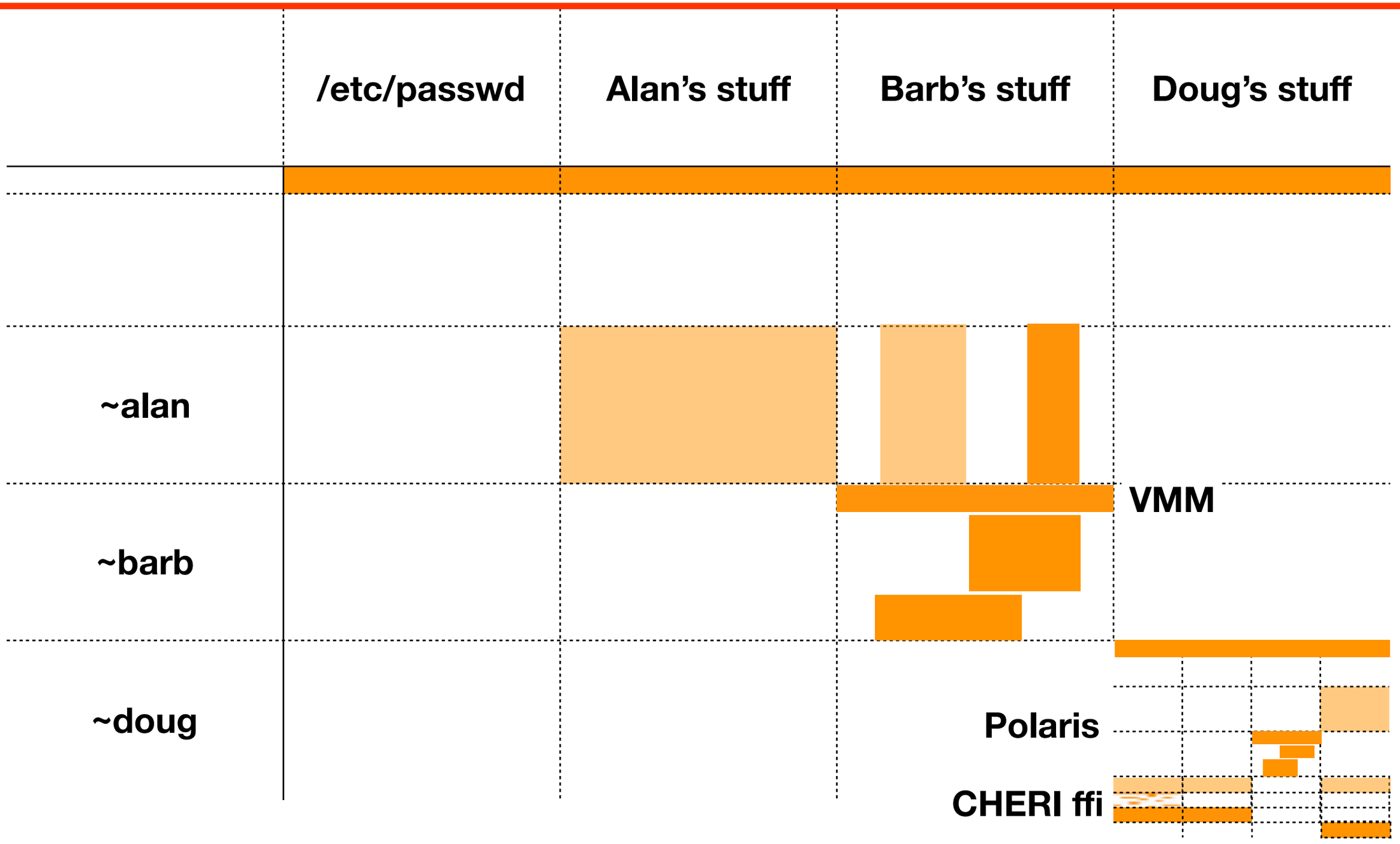
Reduce density
Apply POLA recursively



Reduce height
Minimize+verify each TCB



Reduce width
Partition virtualized legacy



Multiplicative risk reduction

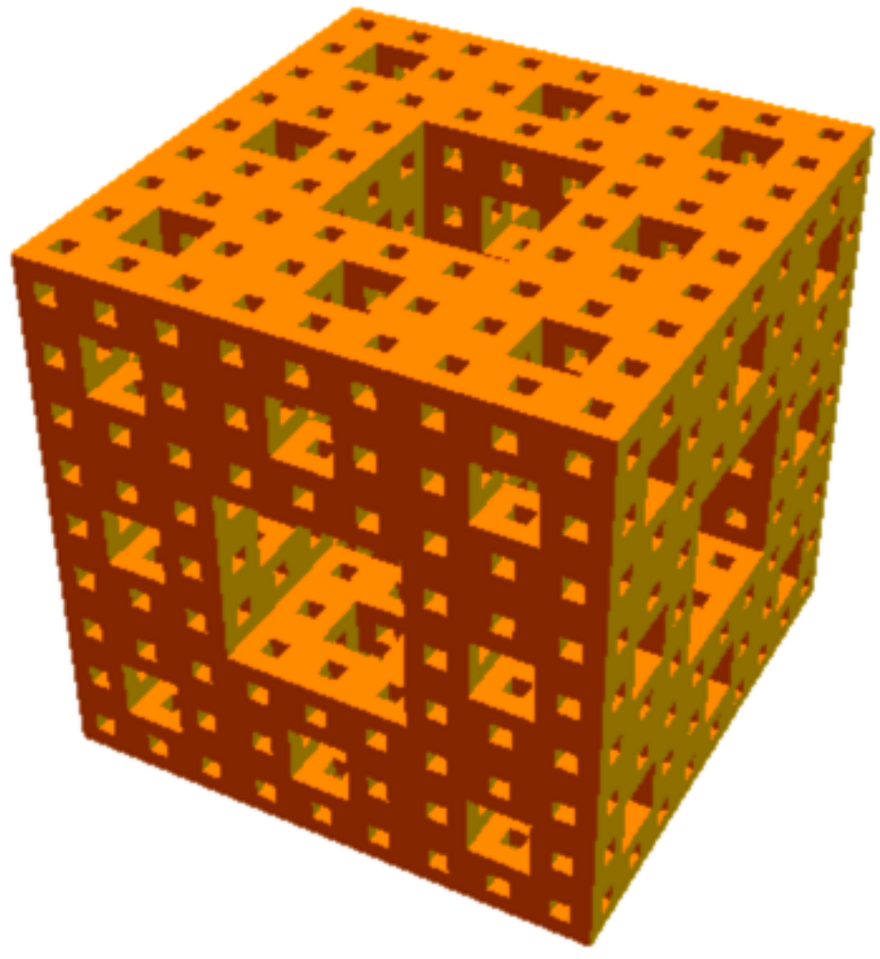
Reduce horizontal space	POLA
Reduce density	Composition across scales
Reduce height	Minimize TCBs: μkernel, lang, …
Reduce width	Compositional virtualization

Choose Verification Battles

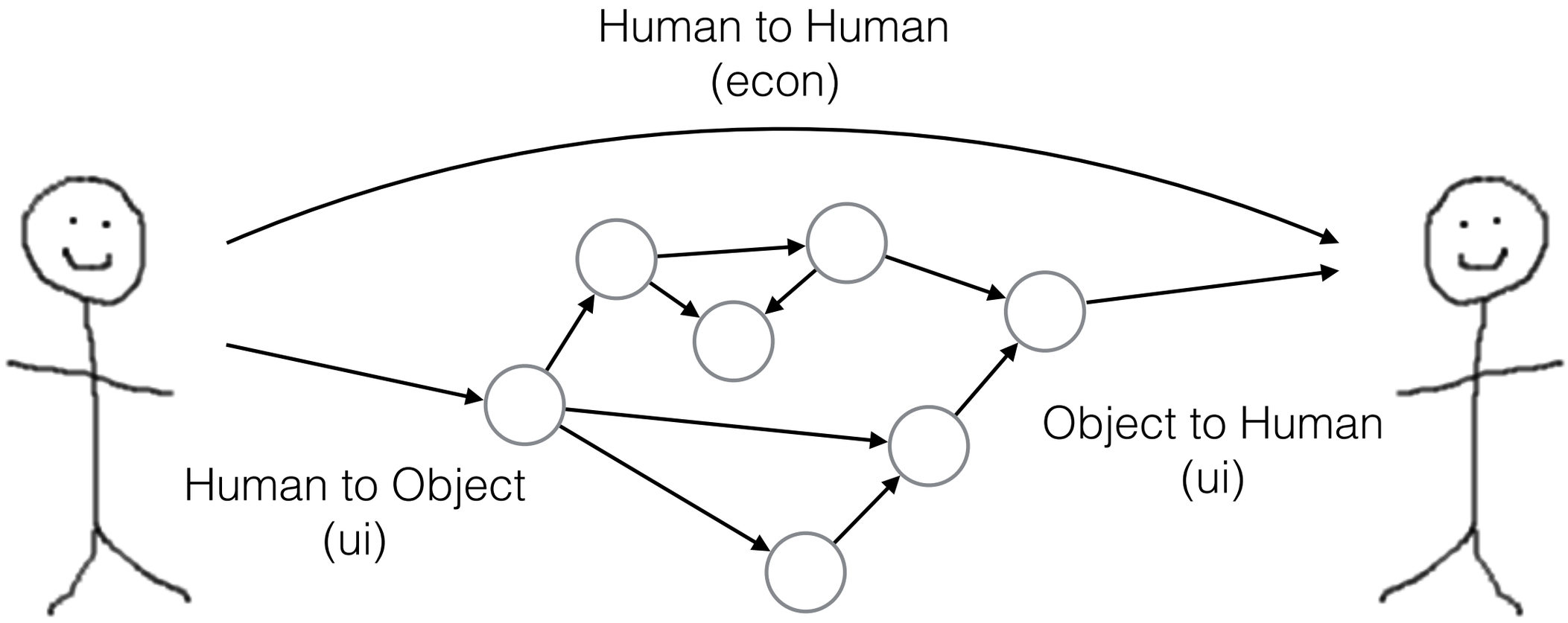
Reduce horizontal space	POLA Patterns limit authority?
Reduce density	Composition across scales Embedding preserves security?
Reduce height	Minimize TCBs: μkernel, lang, … **Formal verification**
Reduce width	Compositional virtualization Impenetrable confinement?

Substrate	Historical System	System
Hardware	CMNM, Plessey 250, C.mmp, CM*, CAP, Flex, IBM System/38, Intel 432	Crash-SAFE, **CHERI**, Risc-V
OS	DVH, Hydra, StarOS, RATS, Cal-TSS, PSOS, NLTSS, Spring	**Capsicum**, CloudABI, Genode, Barrelfish, Fuchsia
KeyKOS family OS	Gnosis, KeyKOS, GuardOS, EROS, CapROS, Coyotos	**seL4**
Distributed OS	Ameoba, Mach, Midori	
Language	Gedanken, W7, J-Kernel, Joe-E, Emily, CaPerl, **Caja**, Tamed Pict, Plash	**Monte**, **Frozen Realms**, shill, Wyvern, **wasm-gc**
Distributed Language	Act-1, Eden, Emerald, Vulcan, Joule, E, Oz-E, M#	**Pony**, Kappa, **Dr.SES**
Distributed Storage	Scoopfs	Tahoe-LAFS
Crypto Protocol	DCCS, CapTP, Foolscap, Client Utility, **Waterken**	COAST, **Cap'n Proto**
Offline Certs	SPKI/SDSI, E-Speak, CapCert	Macaroons, **Id-ocap**
Blockchain		**Gravity**, **Dfinity**, **RChain**, Cosmos, **Veres One**, Sovrin, **Agoric Systems**
User Interface	CapDesk, Scoopfs, **Belay**	**Sandstorm**

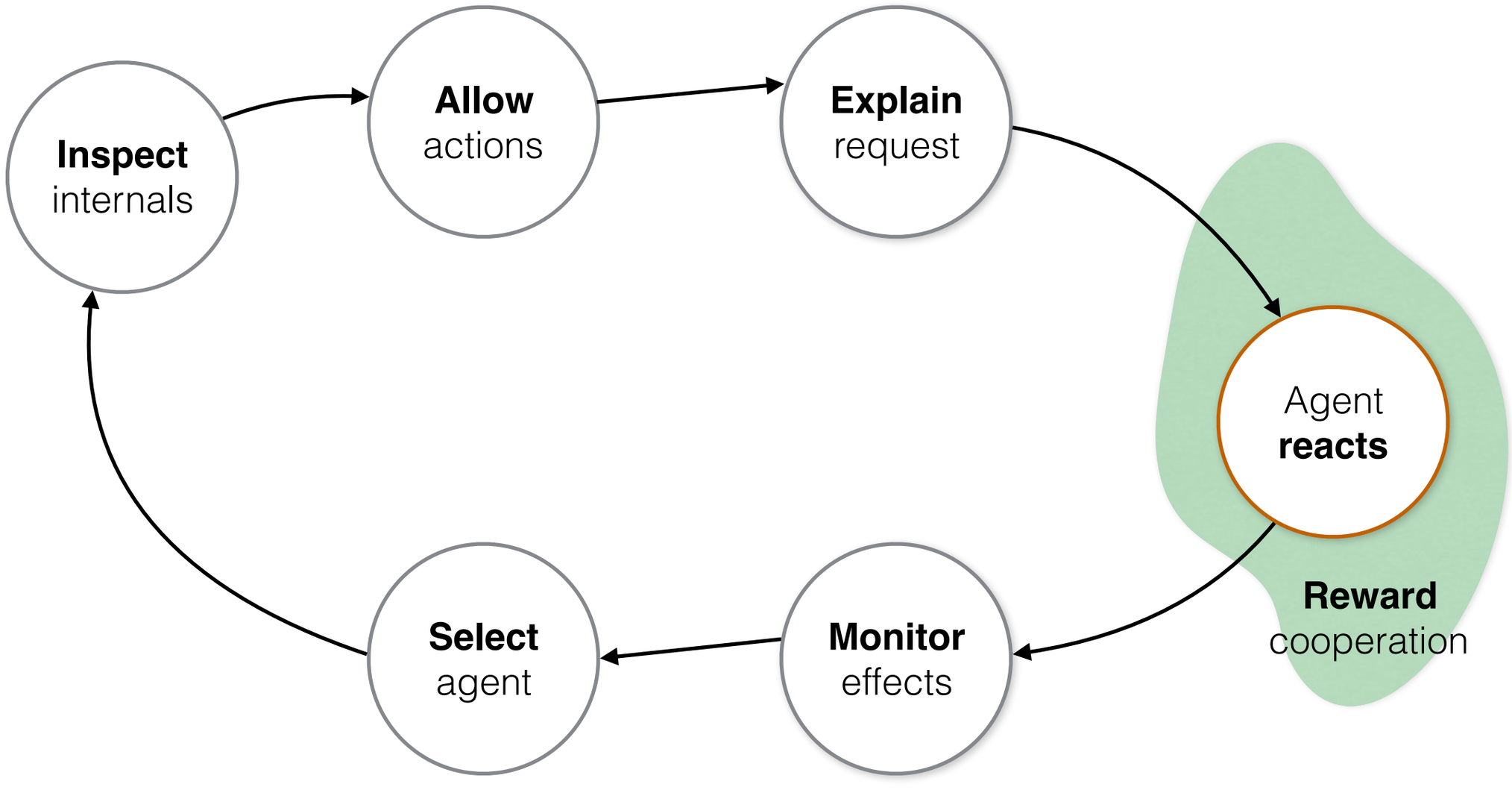
Questions?



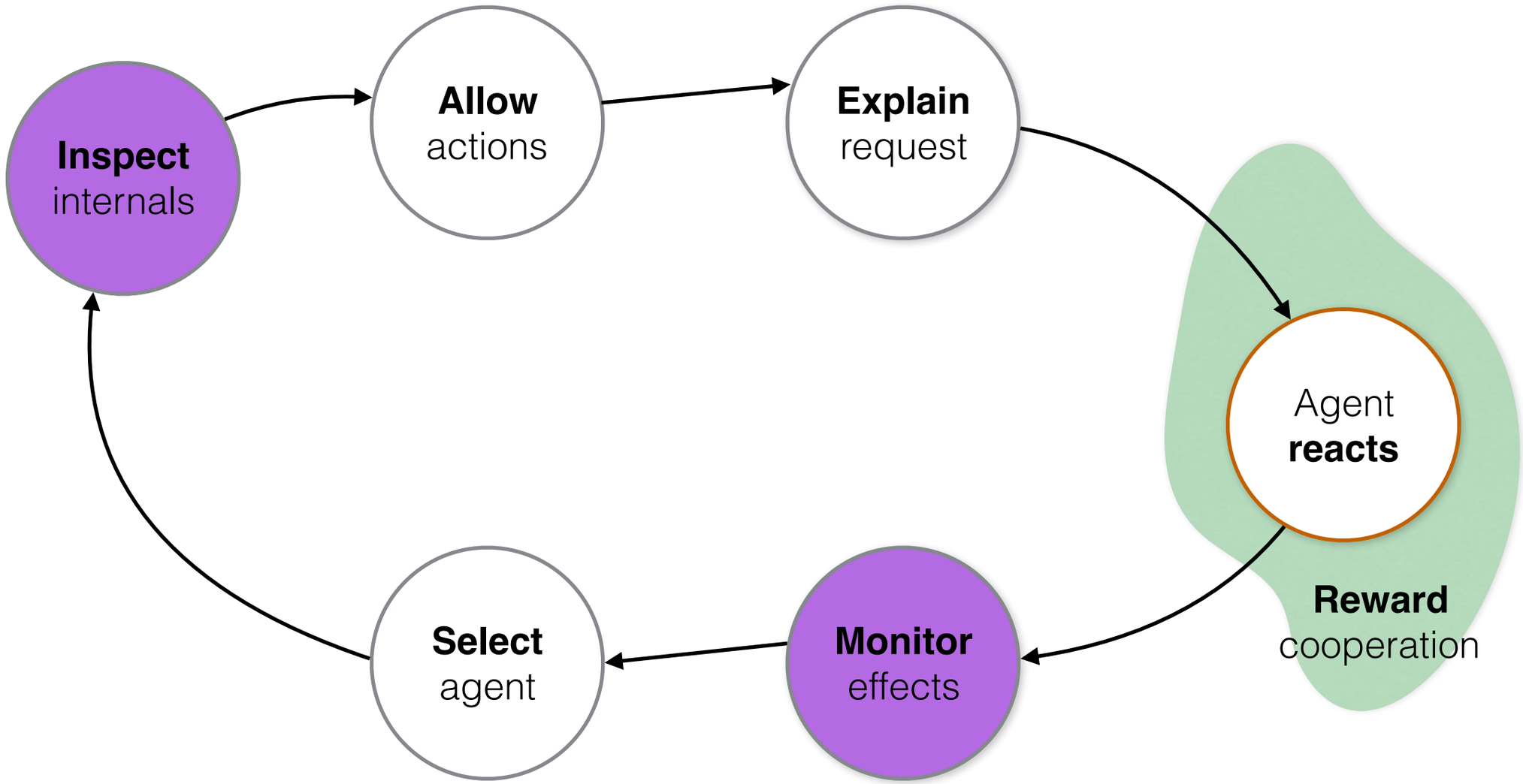
Networks of request making



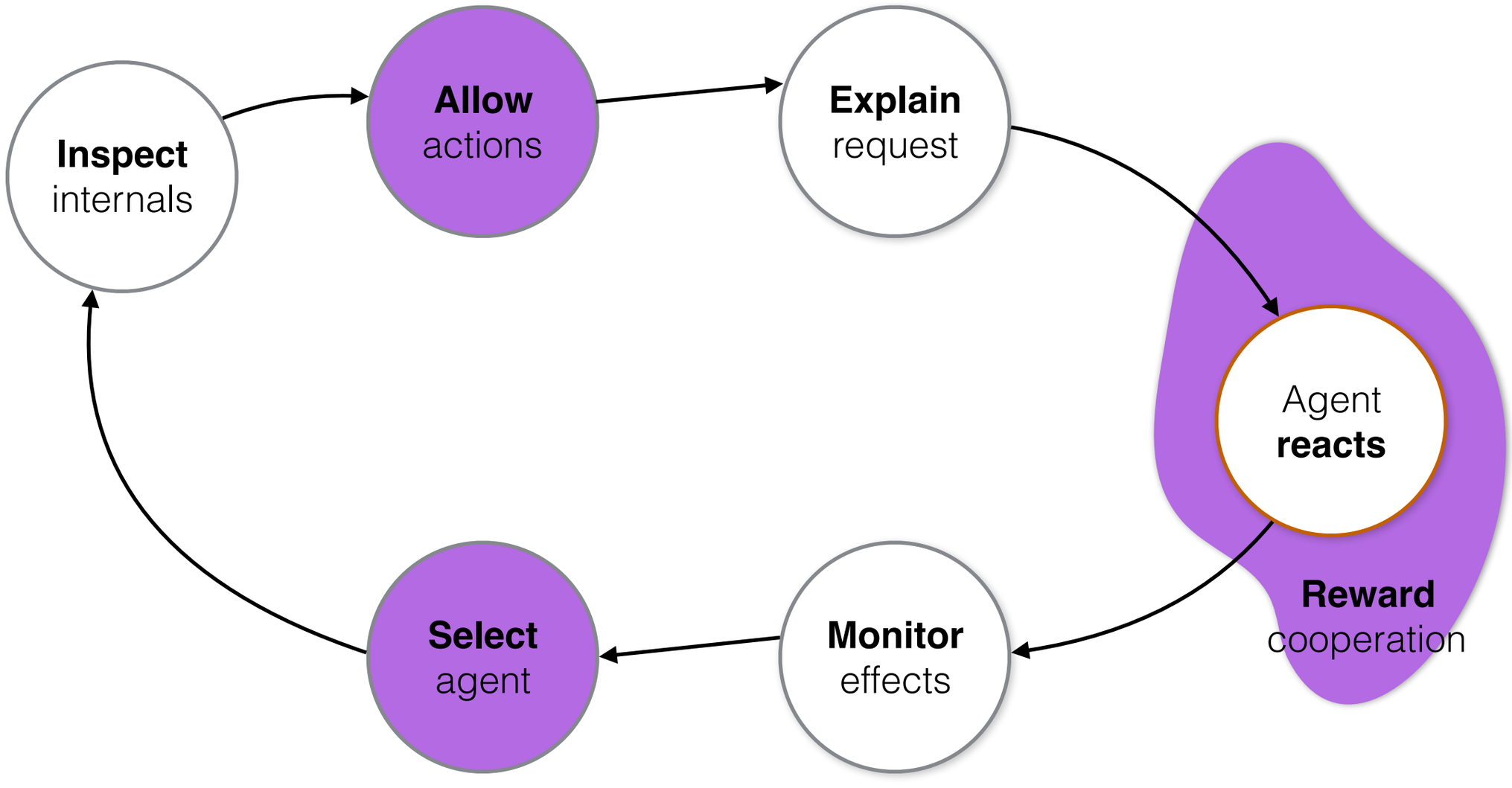
The Principal-Agent Loop



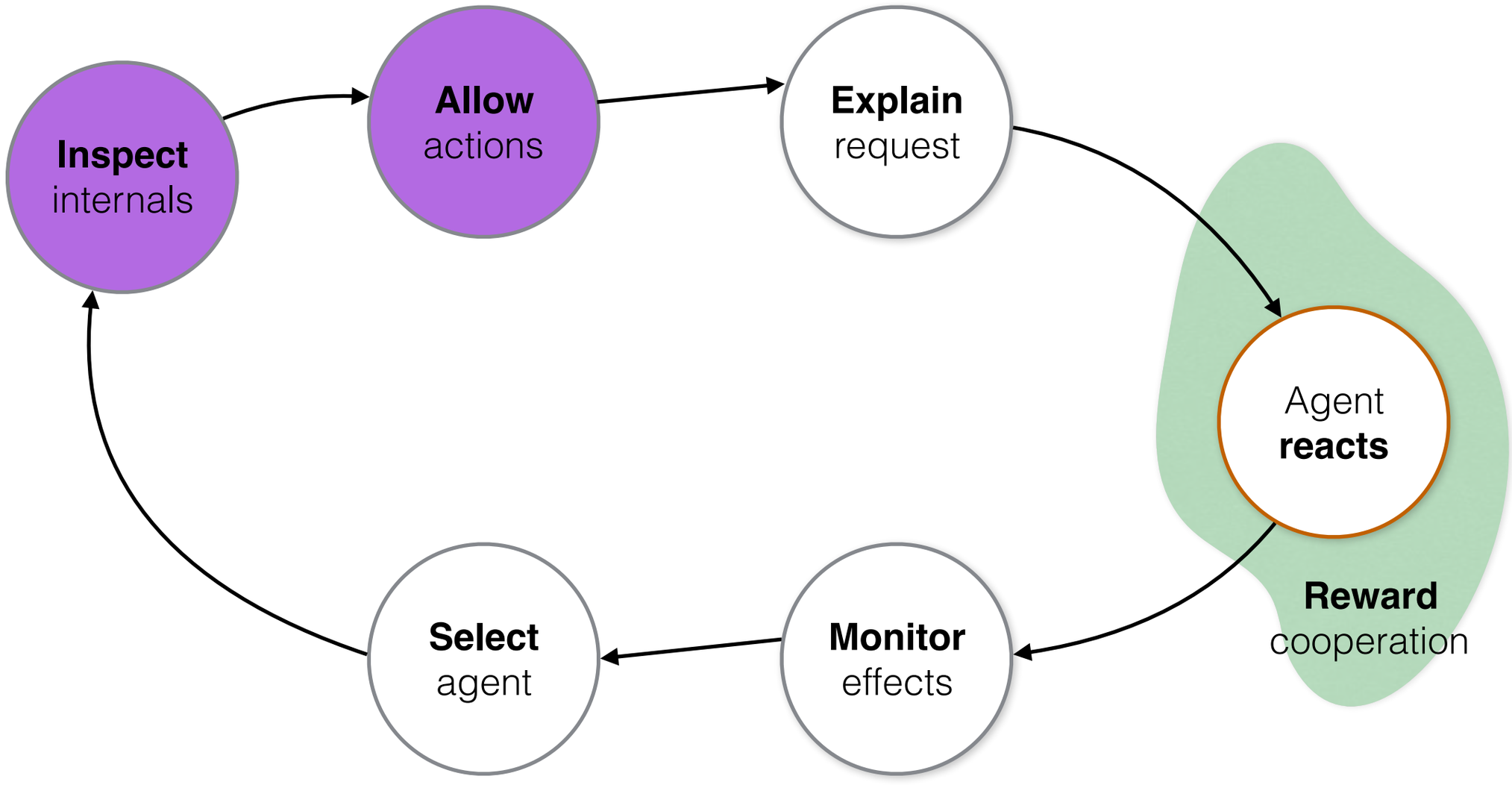
The Principal-Agent Loop



The Principal-Agent Loop



The Principal-Agent Loop



The Elements of Decision Alignment

	Human to Human	Human to/from Object	Object to Object
Select agent	Trademark Chain of custody	App stores White and black lists	Trusted developer Same origin
Inspect internals	Accounting controls	Trusted path URL bar	Types, Verification Open source eyeballs
Allow actions	Law, Contracts	App permissions Powerbox	Security Protection patterns
Explain request	Language	User interface	Abstraction
Reward cooperation	Economics Incentive Alignment	Objective functions	Machine learning Agorics
Monitor effects	Reviews, Complaints Word of mouth	Bug reports	Contracts, Testing Backprop

The Elements of Decision Alignment

	Human to Human	Human to/from Object	Object to Object
Select agent	Trademark Chain of custody	App stores White and black lists	Trusted developer Same origin
Inspect internals	Accounting controls	Trusted path URL bar	Types, **Verification** Open source eyeballs
Allow actions	Law, Contracts	App permissions Powerbox	Security **Protection patterns**
Explain request	Language	User interface	Abstraction
Reward cooperation	Economics Incentive Alignment	Objective functions	Machine learning Agorics
Monitor effects	Reviews, Complaints Word of mouth	Bug reports	Contracts, Testing Backprop

The Elements of Decision Alignment

	Human to Human	Human to/from Object	Object to Object
Select agent	Trademark Chain of custody	App stores White and black lists	Trusted developer Same origin
Inspect internals	Accounting controls	Trusted path URL bar	Types, Verification **Open source eyeballs**
Allow actions	Law, Contracts	App permissions Powerbox	Security Protection patterns
Explain request	Language	User interface	Abstraction
Reward cooperation	Economics Incentive Alignment	Objective functions	Machine learning Agorics
Monitor effects	Reviews, Complaints Word of mouth	Bug reports	Contracts, **Testing** Backprop

The Elements of Decision Alignment

	Human to Human	Human to/from Object	Object to Object
Select agent	Trademark Chain of custody	App stores White and black lists	Trusted developer Same origin
Inspect internals	Accounting controls	Trusted path URL bar	Types, Verification Open source eyeballs
Allow actions	**Law**, Contracts	App permissions Powerbox	Security Protection patterns
Explain request	Language	User interface	Abstraction
Reward cooperation	Economics **Incentive Alignment**	Objective functions	Machine learning Agorics
Monitor effects	Reviews, Complaints Word of mouth	Bug reports	Contracts, Testing Backprop

The Elements of Decision Alignment

	Human to Human	Human to/from Object	Object to Object
Select agent	Trademark Chain of custody	App stores White and black lists	Trusted developer Same origin
Inspect internals	Accounting controls	Trusted path URL bar	Types, Verification Open source eyeballs
Allow actions	Law, Contracts	App permissions Powerbox	Security **Protection patterns**
Explain request	Language	User interface	Abstraction
Reward cooperation	Economics **Incentive Alignment**	Objective functions	Machine learning Agorics
Monitor effects	Reviews, Complaints Word of mouth	Bug reports	Contracts, Testing Backprop

The Elements of Decision Alignment

	Human to Human	Human to/from Object	Object to Object
Select agent	Trademark Chain of custody	App stores White and black lists	Trusted developer Same origin
Inspect internals	Accounting controls	Trusted path URL bar	Types, **Verification** Open source eyeballs
Allow actions	Law, Contracts	App permissions Powerbox	Security **Protection patterns**
Explain request	Language	User interface	Abstraction
Reward cooperation	Economics Incentive Alignment	Objective functions	Machine learning Agorics
Monitor effects	Reviews, Complaints Word of mouth	Bug reports	Contracts, Testing Backprop

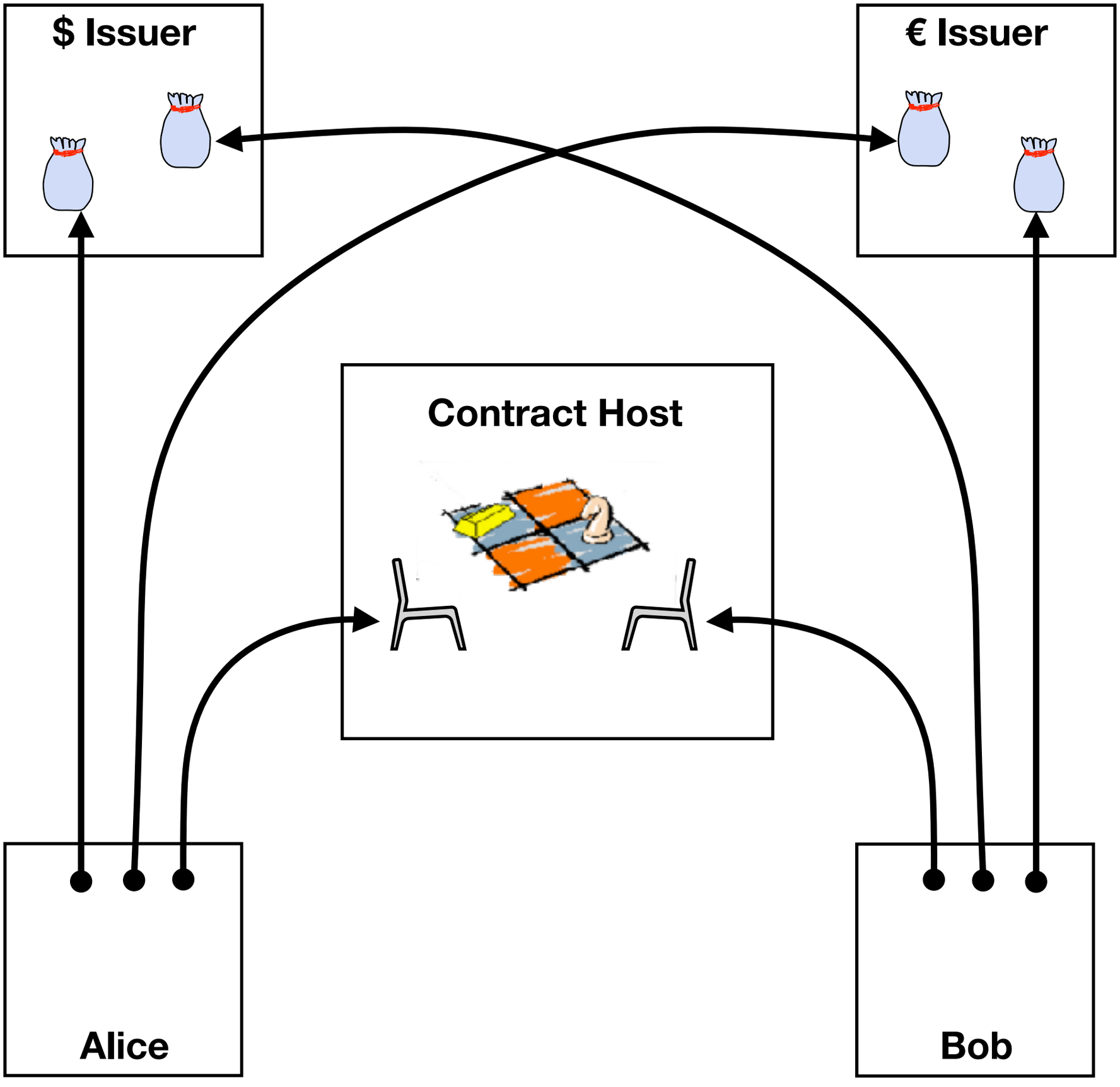
Escrow Exchange Contract

```
function escrowExchange(a, b) {                          // a from Alice, b from Bob
  let decide;
  const decisionP = new Promise(resolve => { decide = resolve; });

  function transfer(srcPurseP, dstPurseP, amount) {
    const makeEscrowPurseP = Q.join(srcPurseP ! makePurse,
                                    dstPurseP ! makePurse);
    const escrowPurseP = makeEscrowPurseP ! ();
    Q(decisionP).then(                                   // setup phase 2
      _ => dstPurseP ! deposit(amount, escrowPurseP); },
      _ => srcPurseP ! deposit(amount, escrowPurseP); });

    return escrowPurseP ! deposit(amount, srcPurseP);    // phase 1
  }
  async function failOnly(cancellationP) { throw await cancellationP; }

  decide(Promise.race([Promise.all([
      transfer(a.moneySrcP, b.moneyDstP, b.moneyNeeded),
      transfer(b.stockSrcP, a.stockDstP, a.stockNeeded)
    ]),
    failOnly(a.cancellationP),
    failOnly(b.cancellationP)]));
  return decisionP;
}
```


$ Issuer
€ Issuer
Contract Host
Alice
Bob

Substrate Independent Cap Logic

Hardware	CAP, C.mmp, IBM Sys38, Intel 432, CHERI
OS	DVH, Hydra, KeyKOS, Capsicum, Midori, seL4
Language	Gedanken, W7, E, Joe-E, Emily, M#, Dr.SES
Crypto Protocol	DCCS, CapTP, Foolscap, Waterken, Cap'n Proto
Offline Certs	SPKI/SDSI, CapCert, Macaroons, ld-ocap
Blockchain	Gravity, Dfinity, RChain, Cosmos, Agoric Systems
User Interface	CapDesk, Belay, Sandstorm

Substrate Independent Cap Logic

Hardware	CAP, C.mmp, IBM Sys38, Intel 432, **CHERI**
OS	DVH, Hydra, KeyKOS, **Capsicum, Midori, seL4**
Language	Gedanken, W7, E, Joe-E, Emily, **M#, Dr.SES**
Crypto Protocol	DCCS, CapTP, Foolscap, **Waterken, Cap'n Proto**
Offline Certs	SPKI/SDSI, CapCert, **Macaroons, ld-ocap**
Blockchain	**Gravity, Dfinity, RChain, Cosmos, Agoric Systems**
User Interface	CapDesk, Belay, **Sandstorm**