Into the MPCVD Multiverse

Exploring the hyperdimensional geometry of possible CVD histories

Allen Householder

CERT/CC

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM21-0441

MOTIVATION

Multi-party Coordinated Vulnerability Disclosure (MPCVD) is increasingly important to critical infrastructure cybersecurity

More organizations are interested in doing it well

How do we know if we're doing a good job at MPCVD?

AGENDA

Into the MPCVD Multiverse

Possible Histories of CVD

Structure of CVD states

Measuring skill in CVD

Extending metrics to MPCVD

Applications

AGENDA

How many ways can this thing go?

Possible Histories of CVD

Structure of CVD states

Measuring skill in CVD

Extending metrics to MPCVD

Applications

6 3 70

12 32 5

6

EVENTS

VENDOR AWARE

PUBLIC AWARE

FIX READY

EXPLOIT PUBLIC

FIX DEPLOYED

ATTACKS OBSERVED

VENDOR AWARE

PUBLIC AWARE

FIX READY

EXPLOIT PUBLIC

FIX DEPLOYED

ATTACKS OBSERVED

3 RULES

$$V \prec F \prec D$$

$$V \prec P \text{ or } P \rightarrow V$$

$$P \prec X \text{ or } X \rightarrow P$$

$\prec$ precedes
$\rightarrow$ leads to

70 HISTORIES

EVERY CVD CASE, EVER.

AXPVFD	PVXAFD	VPXAFD	VAPFDX	VFAPXD	VPFXDA	VPFDXA
APVXFD	VPAXFD	PVFAXD	VAFPXD	VPXFDA	VFAPDX	VFPXDA
AVXPFD	PVAFXD	VXPFAD	PVXFDA	PVFXDA	VFPXAD	VFADPX
XPVAFD	VXPAFD	VPAFXD	VPFAXD	VAFPDX	AVFDPX	VFPDAX
VAXPFD	AVPFXD	VAFXPD	VFAXPD	VPFADX	PVFDXA	VFDAXP
PVAXFD	APVFDX	PVAFDX	VXPFDA	VFPAXD	VPFDAX	VFPDXA
AVPXFD	VAPFXD	AVPFDX	PVFADX	VFXPAD	VFXPDA	VFDAPX
APVFXD	XPVFDA	AVFPXD	VPAFDX	AVFDXP	VFPADX	VFDXPA
XPVFAD	PVXFAD	PVFXAD	VPFXAD	PVFDAX	VAFDPX	VFDPAX
VAPXFD	AVFXPD	VPXFAD	AVFPDX	VAFDXP	VFADXP	VFDPXA

12

ORDER PREFERENCES

WHAT DO WE WANT IN A METRIC?

1. N+1 criteria is better than N

A,B,C,D > A,B,C

~~A,B,C,D > C,D,E~~

~~A,B,C,D > E,F,G~~

Only histories whose criteria are superset/subsets of each other are comparable

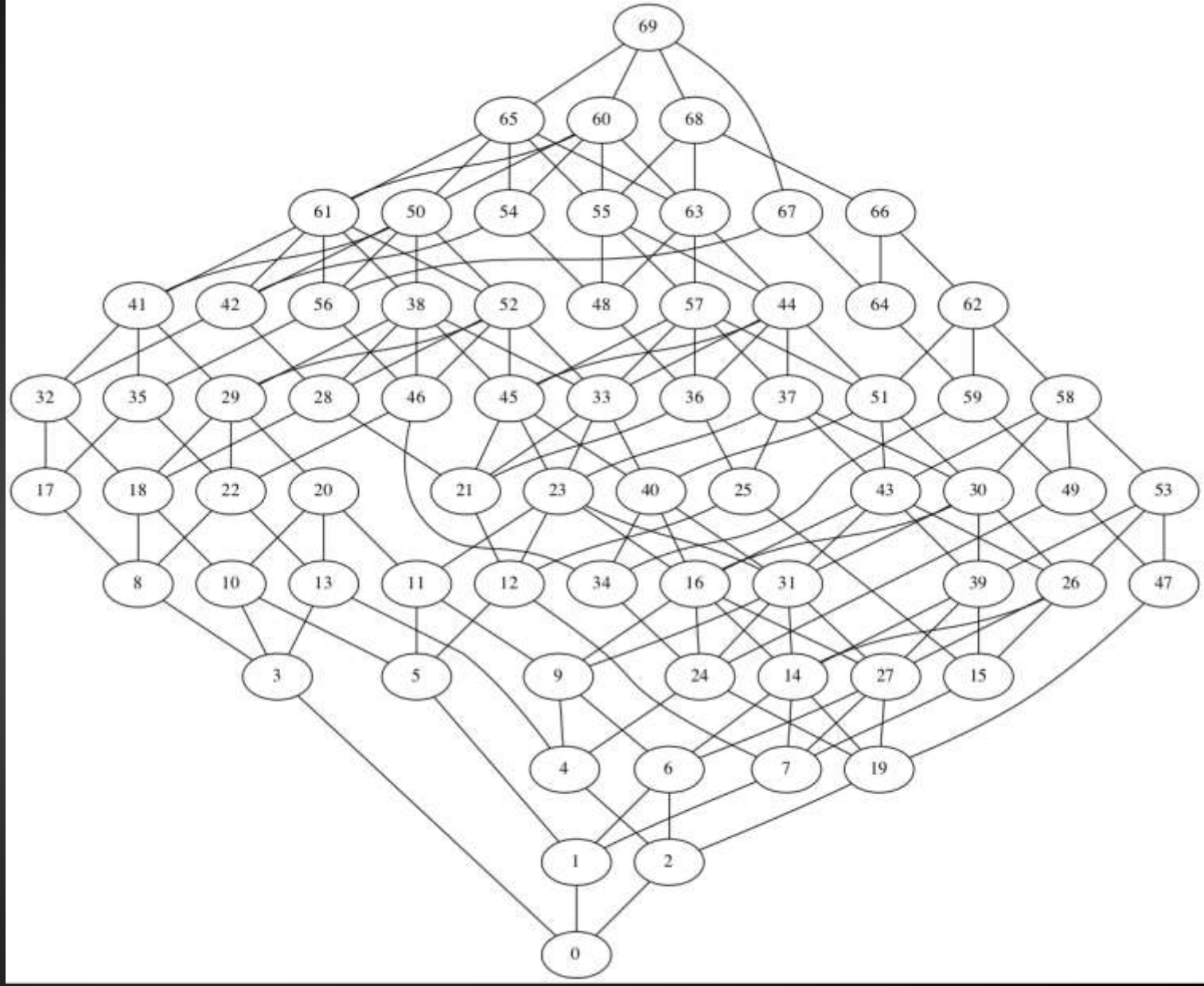
CVD HISTORIES

Partial order over all histories

A>B when

> A MEETS ALL THE SAME CRITERIA AS B PLUS AT LEAST ONE MORE

Histories at the same tier are incomparable



AGENDA

What is the underlying structure of possible case states?

Possible Histories of CVD

Structure of CVD states

Measuring skill in CVD

Extending metrics to MPCVD

Applications

32

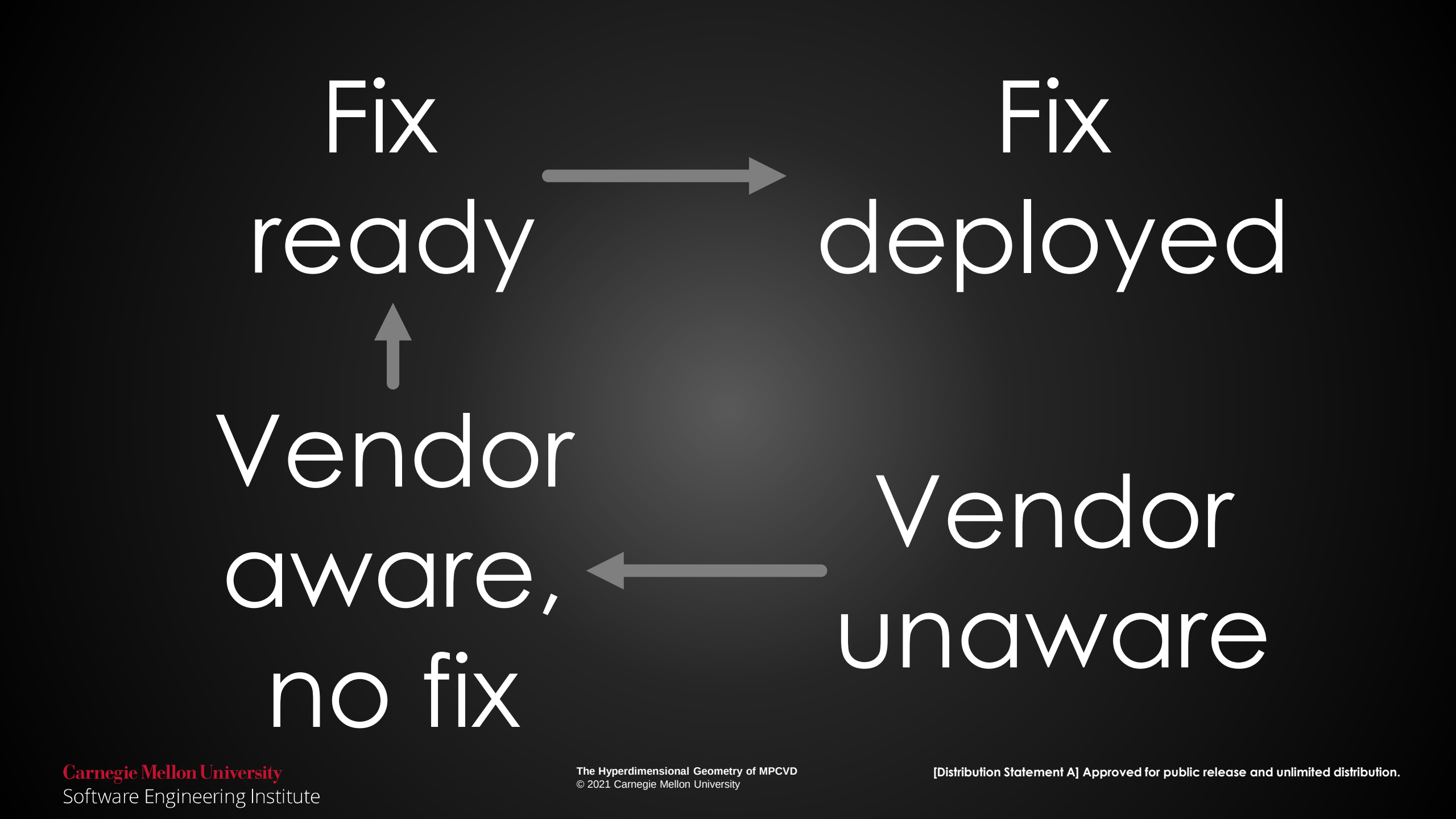
STATES

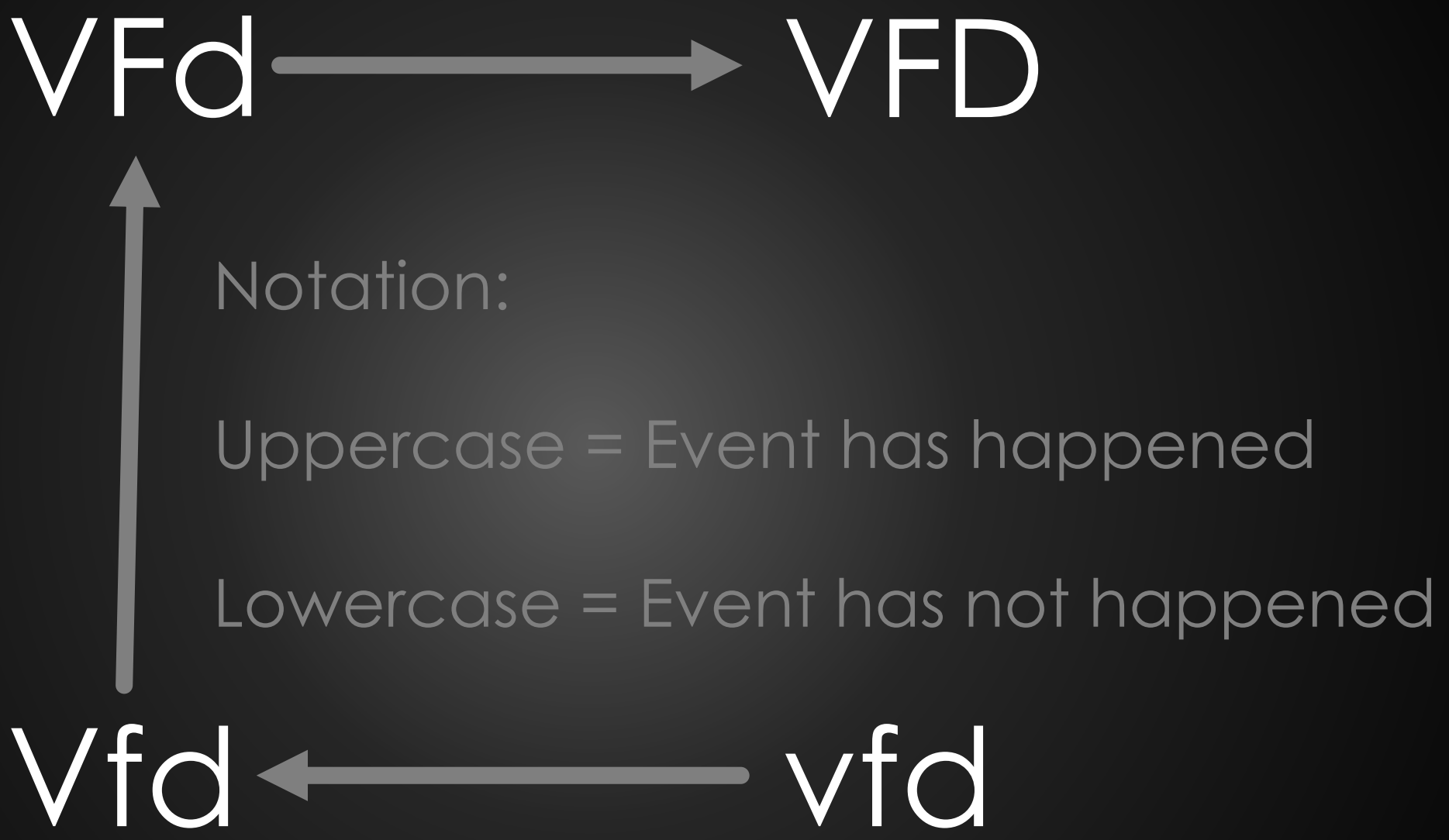
4

X 8

OTHER STATES

FIX PATH STATES





4 X

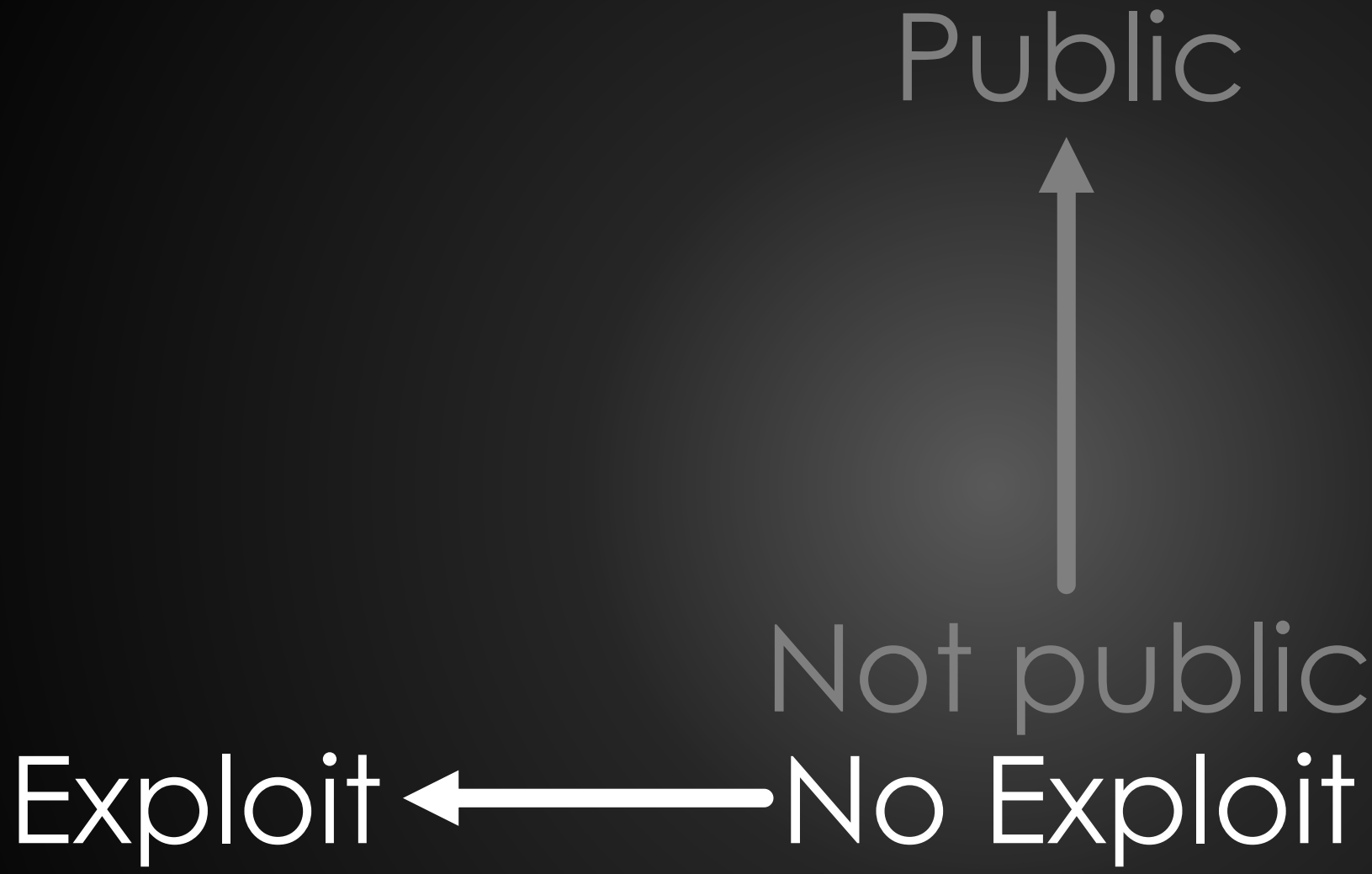
FIX PATH STATES

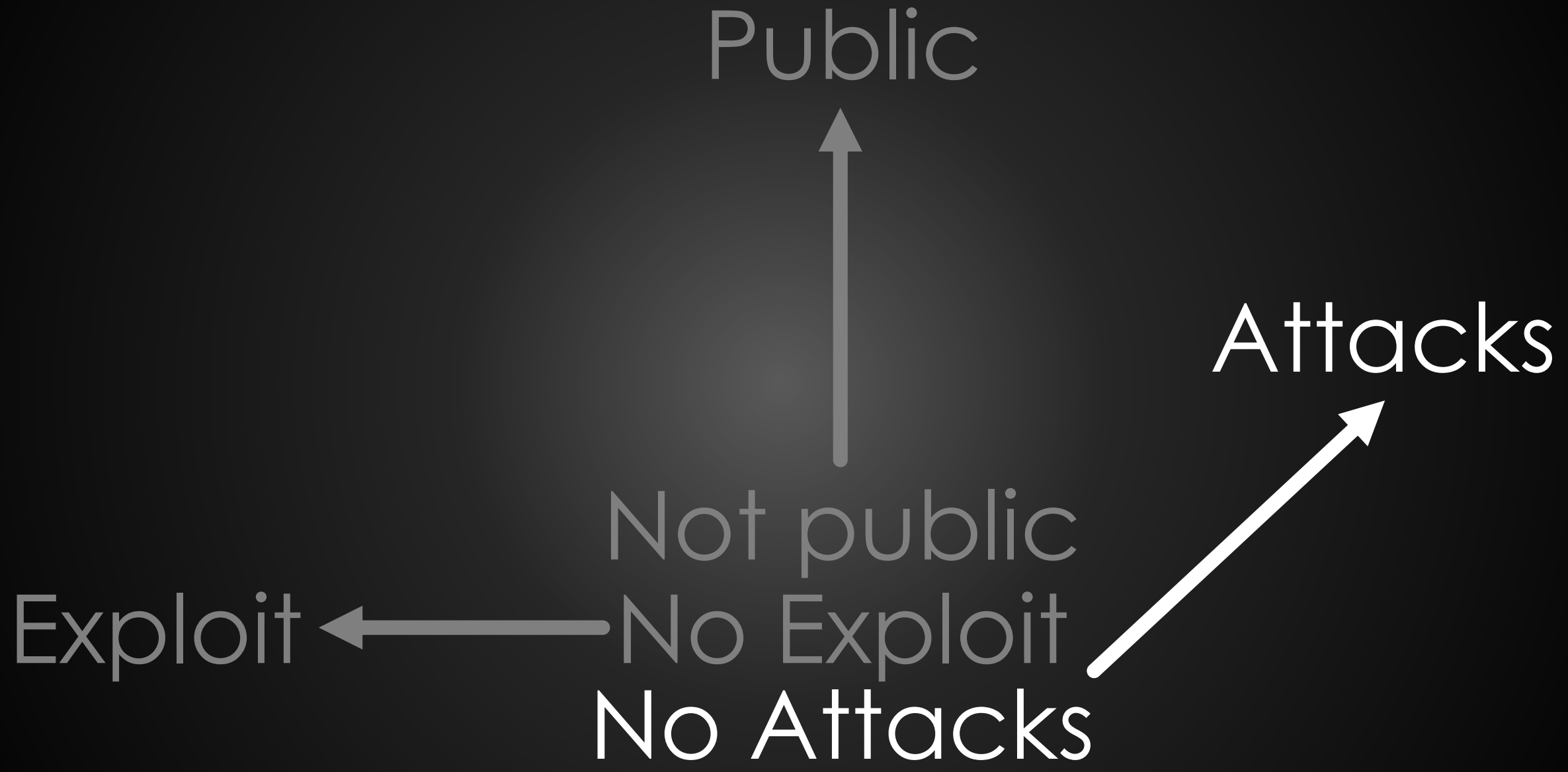
8

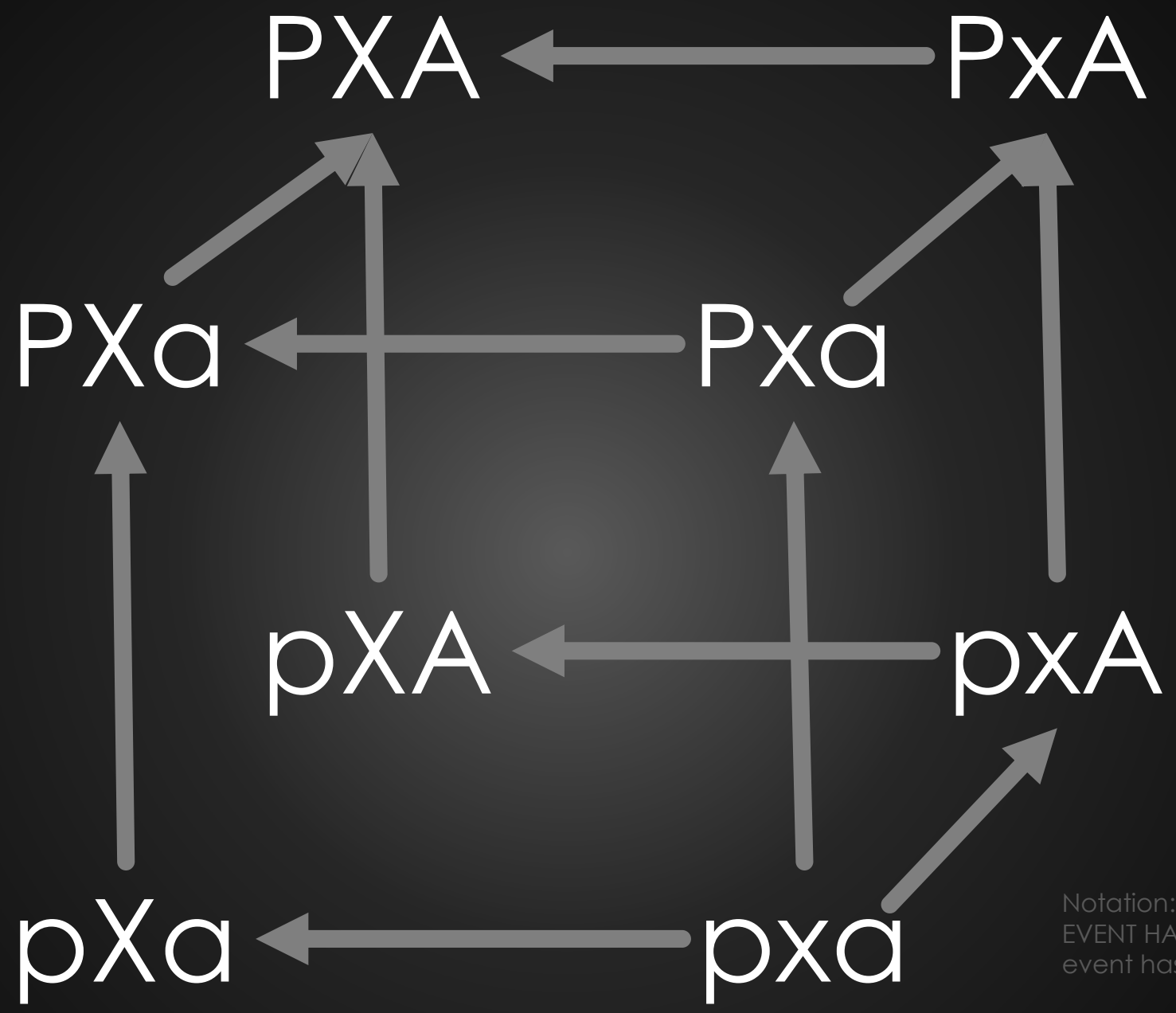
OTHER STATES

Public

Not public





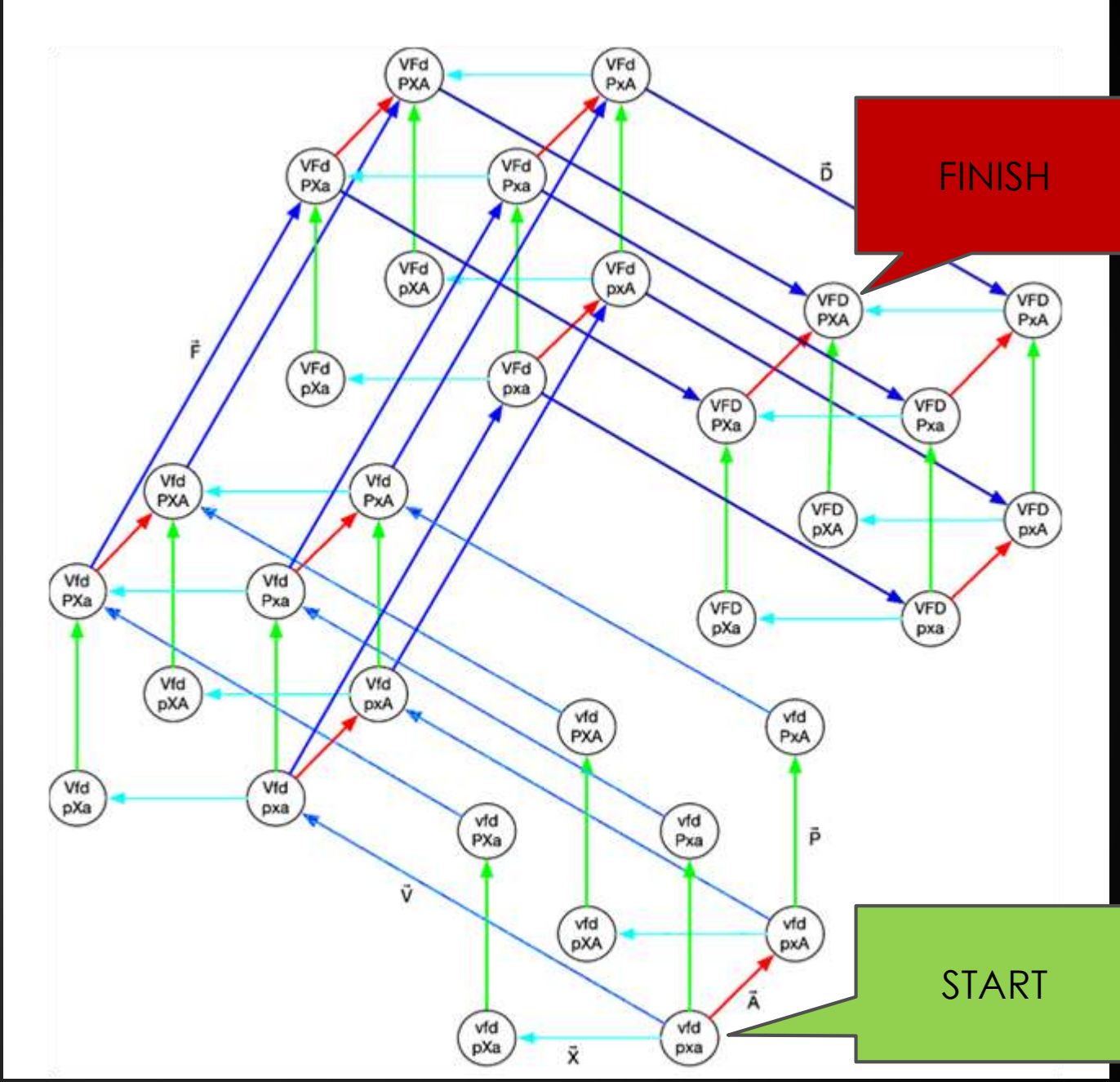


Notation:
EVENT HAS HAPPENED
event has not happened

5 DIMENSIONS

INTRODUCING
THE 5-D CVD HYPERCUBE

- 6 events as state transitions possible as shown
- 3 Rules responsible for missing edges
- 70 possible histories are paths from start to finish
- 12 Desiderata found in paths
- 32 states represent every possible case
- 5 dimensions represents the state space



AGENDA

Are we skillful
or just lucky?

Possible Histories of CVD

Structure of CVD states

Measuring skill in CVD

Extending metrics to MPCVD Applications

WHAT DO WE WANT IN A METRIC?

1. N+1 criteria is better than N
2. Skill is preferable to luck

Maximal Skill

You can hit all 12 desiderata every time

V→F→D→P→X→A every time.

Minimal Skill (Luck)

~~You hit none of them, ever~~

All your success is attributable to luck

ESTIMATING LUCK WITH A RANDOM WALK

vfdpxa →(other states)→ VFDPXA

- Choose from available neighbors with equal probability
- Move to the chosen node
- Count how often the desiderata occur

Assumption:

Events occur with equal probability whenever they are possible

Still only 70 possible histories, just weighted by possible transitions

EXPECTED FREQUENCY OF ROW ≺ COLUMN

ASSUMING EQUIPROBABLE TRANSITIONS

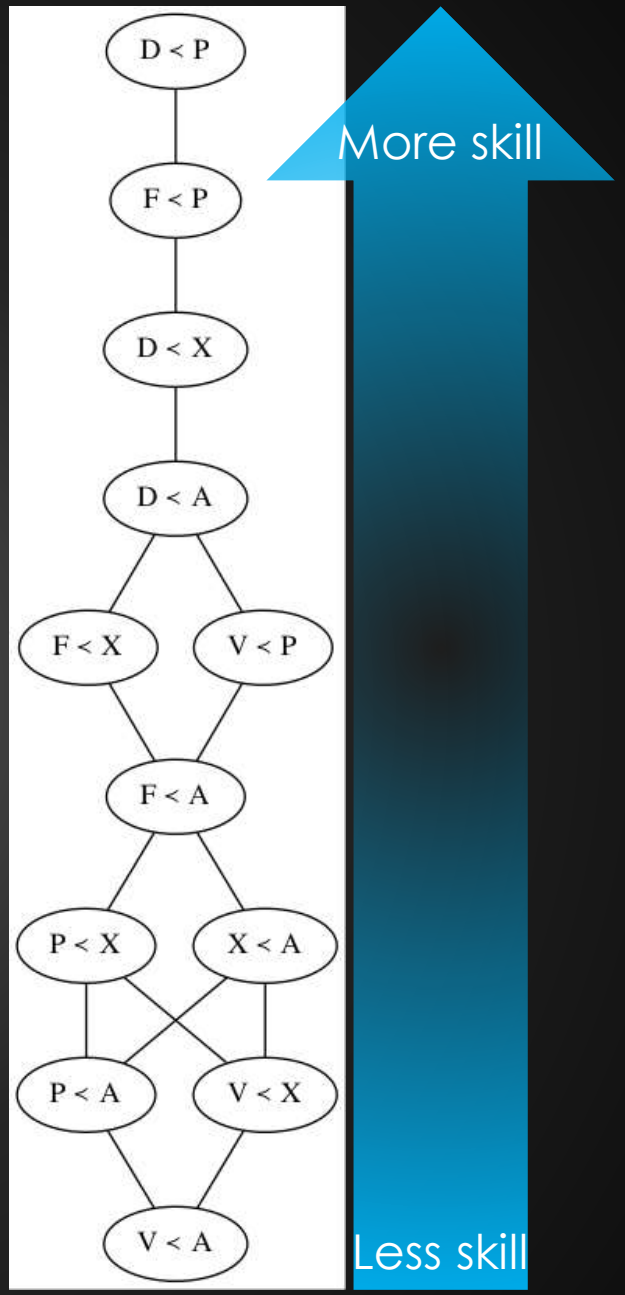
	V	F	D	P	X	A
V	0	1	1	0.333	0.667	0.750
F	0	0	1	0.111	0.333	0.375
D	0	0	0	0.037	0.167	0.187
P	0.667	0.889	0.963	0	0.500	0.667
X	0.333	0.667	0.833	0.500	0	0.500
A	0.250	0.625	0.812	0.333	0.500	0

Less skill

More skill

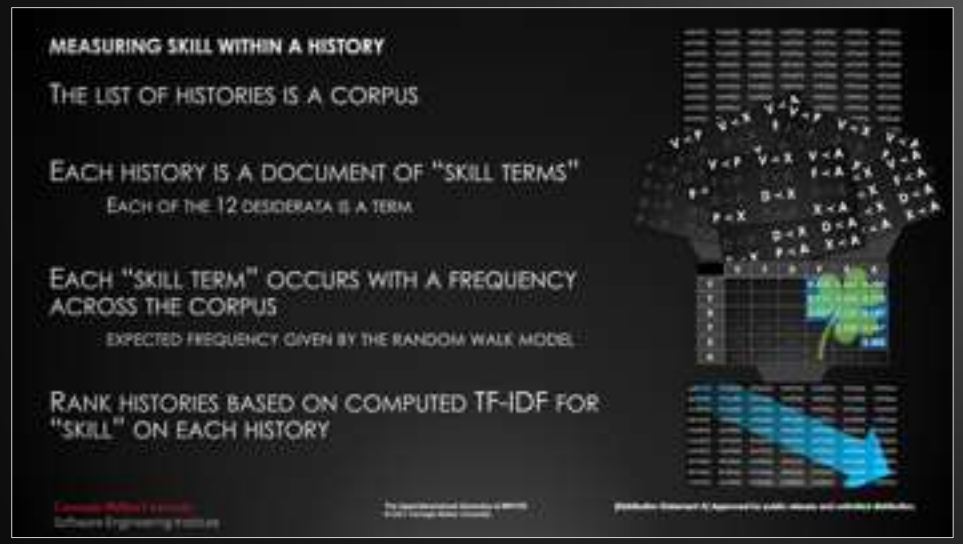
CVD DESIDERATA

Ordered by expected frequency assuming histories generated by a random walk over states

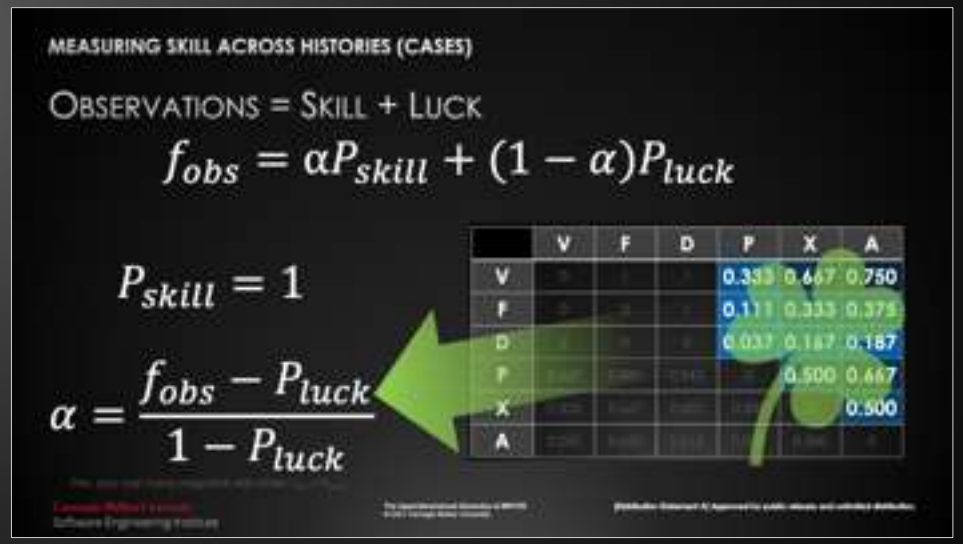


TWO WAYS TO MEASURE CVD SKILL

WITHIN EACH HISTORY



ACROSS OBSERVATIONS



MEASURING SKILL WITHIN A HISTORY

THE LIST OF HISTORIES IS A CORPUS

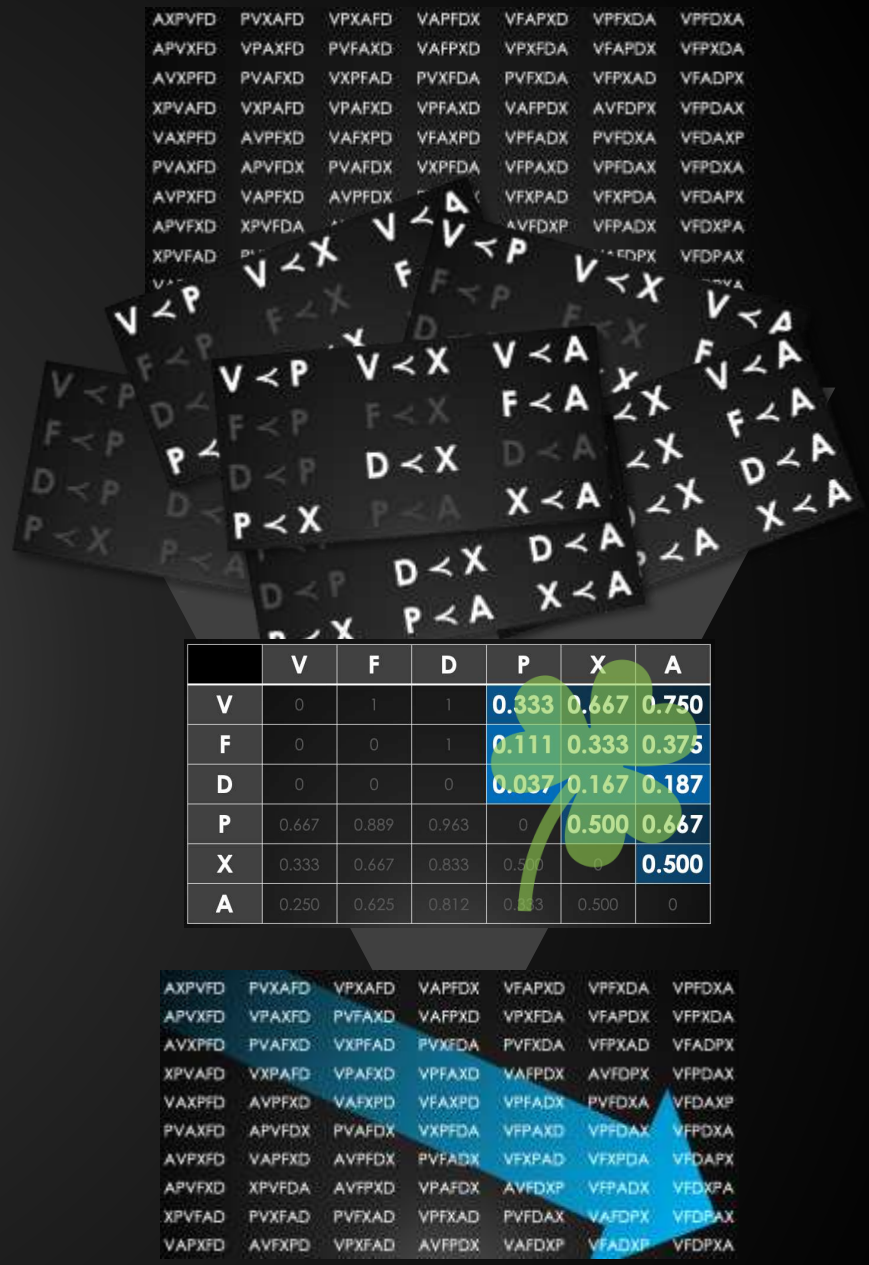
EACH HISTORY IS A DOCUMENT OF "SKILL TERMS"

EACH OF THE 12 DESIDERATA IS A TERM

EACH "SKILL TERM" OCCURS WITH A FREQUENCY ACROSS THE CORPUS

EXPECTED FREQUENCY GIVEN BY THE RANDOM WALK MODEL

RANK HISTORIES BASED ON COMPUTED TF-IDF FOR "SKILL" ON EACH HISTORY



	V	F	D	P	X	A
V	0	1	1	0.333	0.667	0.750
F	0	0	1	0.111	0.333	0.375
D	0	0	0	0.037	0.167	0.187
P	0.667	0.889	0.963	0	0.500	0.667
X	0.333	0.667	0.833	0.500	0	0.500
A	0.250	0.625	0.812	0.333	0.500	0

EVERY CVD CASE, EVER. SKILL INCREASES DOWN AND TO THE RIGHT

AXPVFD	PVXAFD	VPXAFD	VAPFDX	VFAPXD	VPFXDA	VPFDXA
APVXFD	VPAXFD	PVFAXD	VAFPXD	VPXFDA	VFAPDX	VFPXDA
AVXPFD	PVAFXD	VXPFAD	PVXFDA	PVFXDA	VFPXAD	VFADPX
XPVAFD	VXPAFD	VPAFXD	VPFAXD	VAFPDX	AVFDPX	VFPDAX
VAXPFD	AVPFXD	VAFXPD	VFAXPD	VPFADX	PVFDXA	VFDAXP
PVAXFD	APVFDX	PVAFDX	VXPFDA	VFPAXD	VPFDAX	VFPDXA
AVPXFD	VAPFXD	AVPFDX	PVFADX	VFXPAD	VFXPDA	VFDAPX
APVFXD	XPVFDA	AVFPXD	VPAFDX	AVFDXP	VFPADX	VFDXPA
XPVFAD	PVXFAD	PVFXAD	VPFXAD	PVFDAX	VAFDPX	VFDPAX
VAPXFD	AVFXPD	VPXFAD	AVFPDX	VAFDXP	VFADXP	VFDPXA

MEASURING SKILL ACROSS HISTORIES (CASES)

OBSERVATIONS = SKILL + LUCK

$$f_{obs} = \alpha P_{skill} + (1 - \alpha) P_{luck}$$

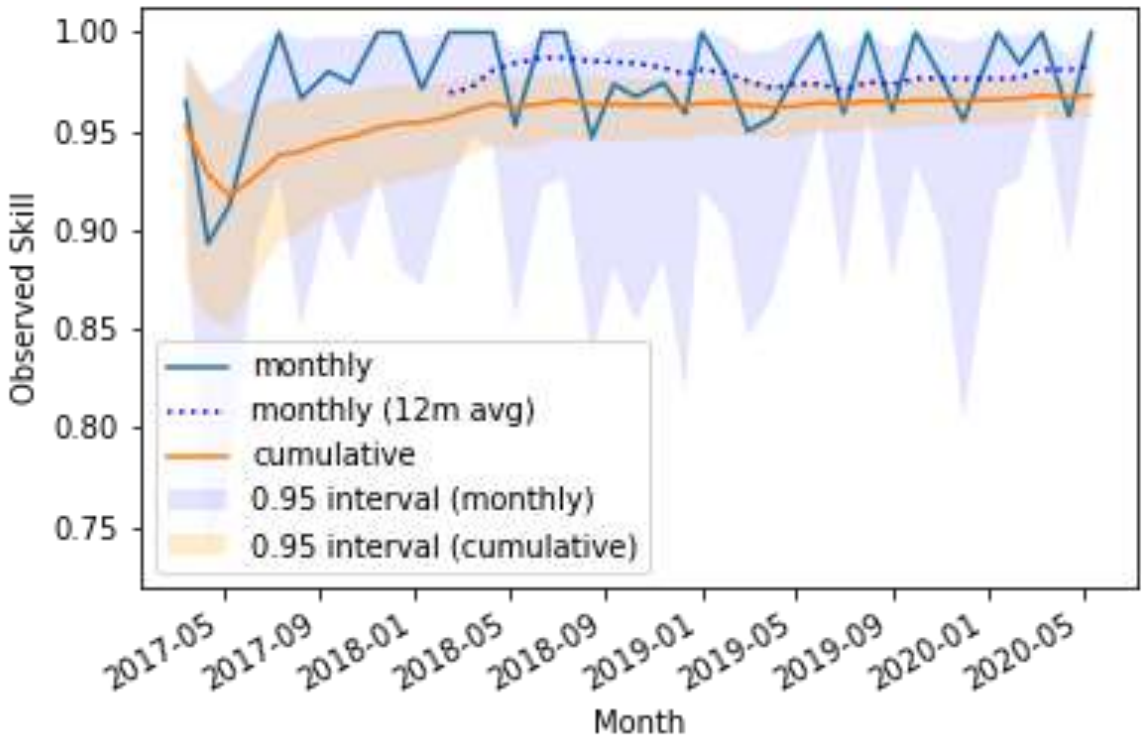
$$P_{skill} = 1$$

$$\alpha = \frac{f_{obs} - P_{luck}}{1 - P_{luck}}$$

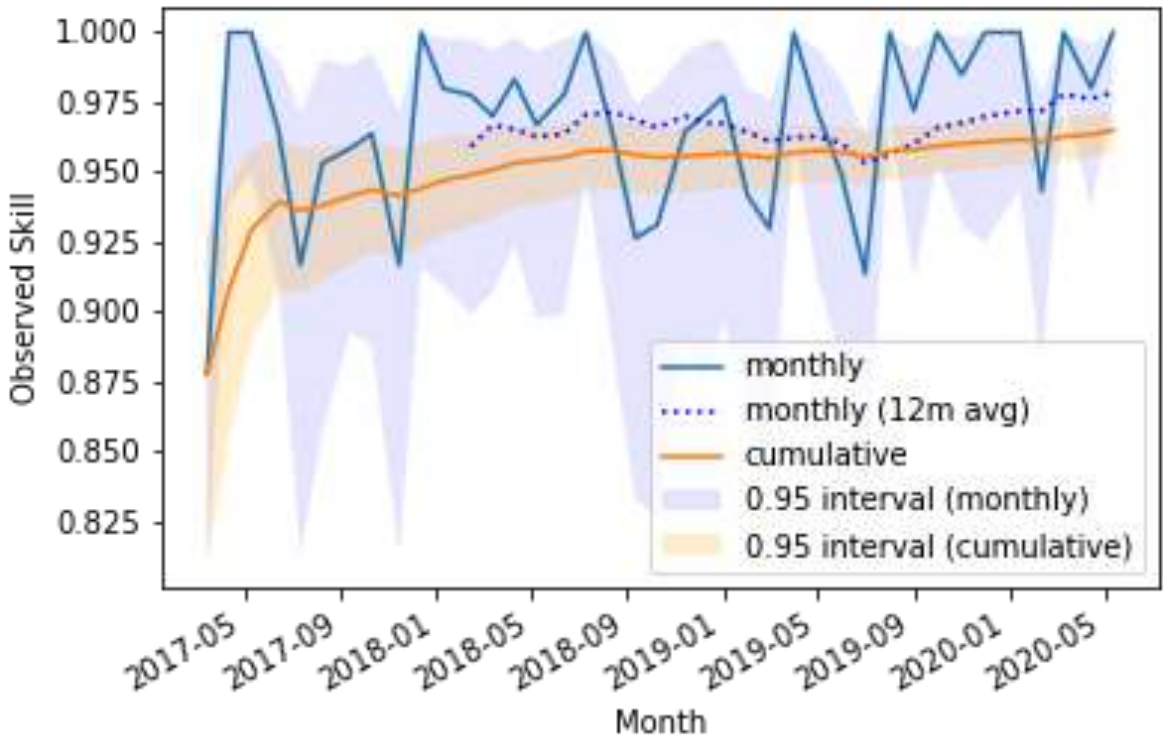
	V	F	D	P	X	A
V	0	1	1	0.333	0.667	0.750
F	0	0	1	0.111	0.333	0.375
D	0	0	0	0.037	0.167	0.187
P	0.667	0.889	0.963	0	0.500	0.667
X	0.333	0.667	0.833	0.500	0	0.500
A	0.250	0.625	0.812	0.333	0.500	0

Yes, you can have negative skill when $f_{obs} < P_{luck}$

Fix Ready before Attacks

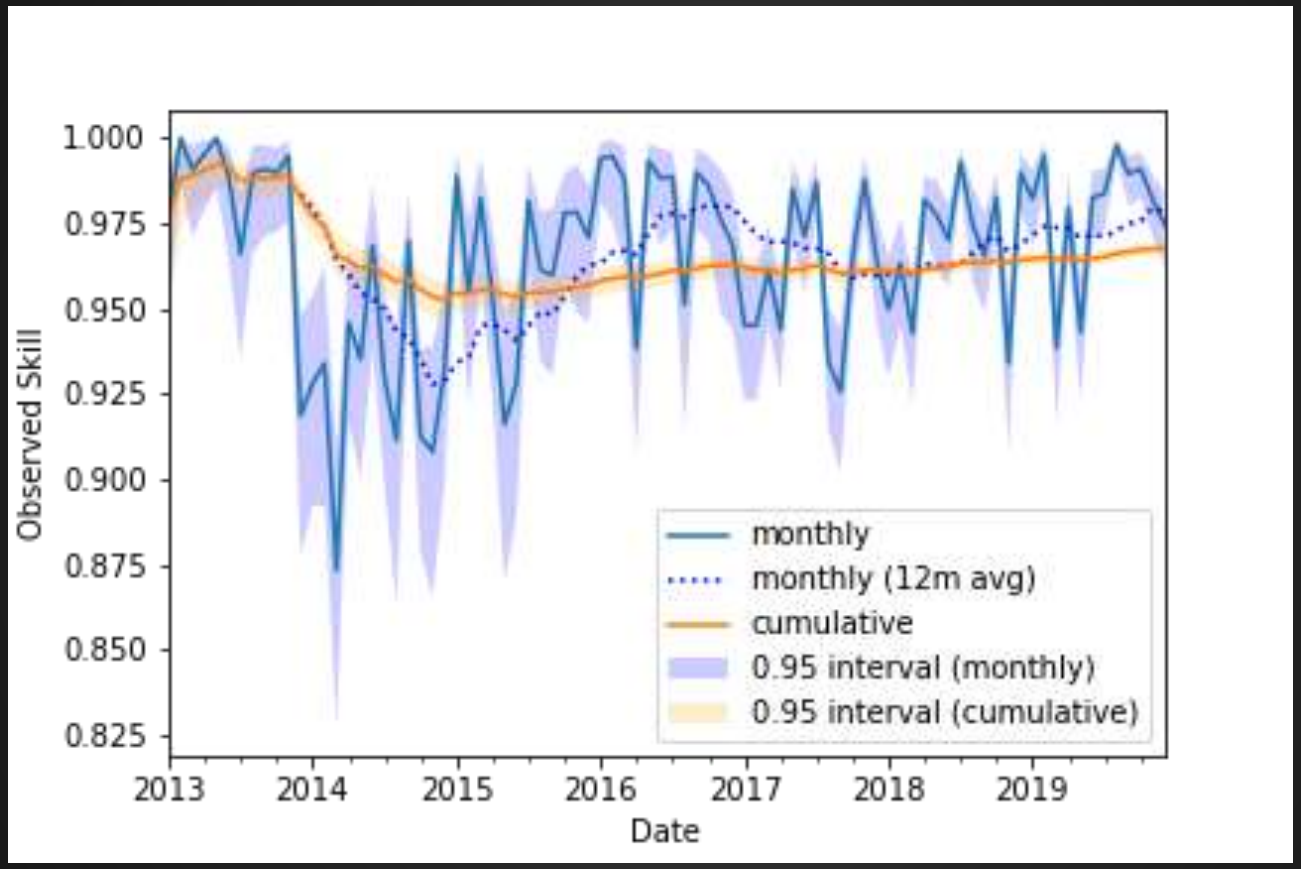


Fix Ready before Public Awareness



Source: Microsoft via ZDI Blog

Public Aware before Exploit Published



Source: NVD, CERT/CC, Metasploit Framework, ExploitDB

AGENDA

Toward macro-scale metrics for MPCVD

Possible Histories of CVD

Structure of CVD states

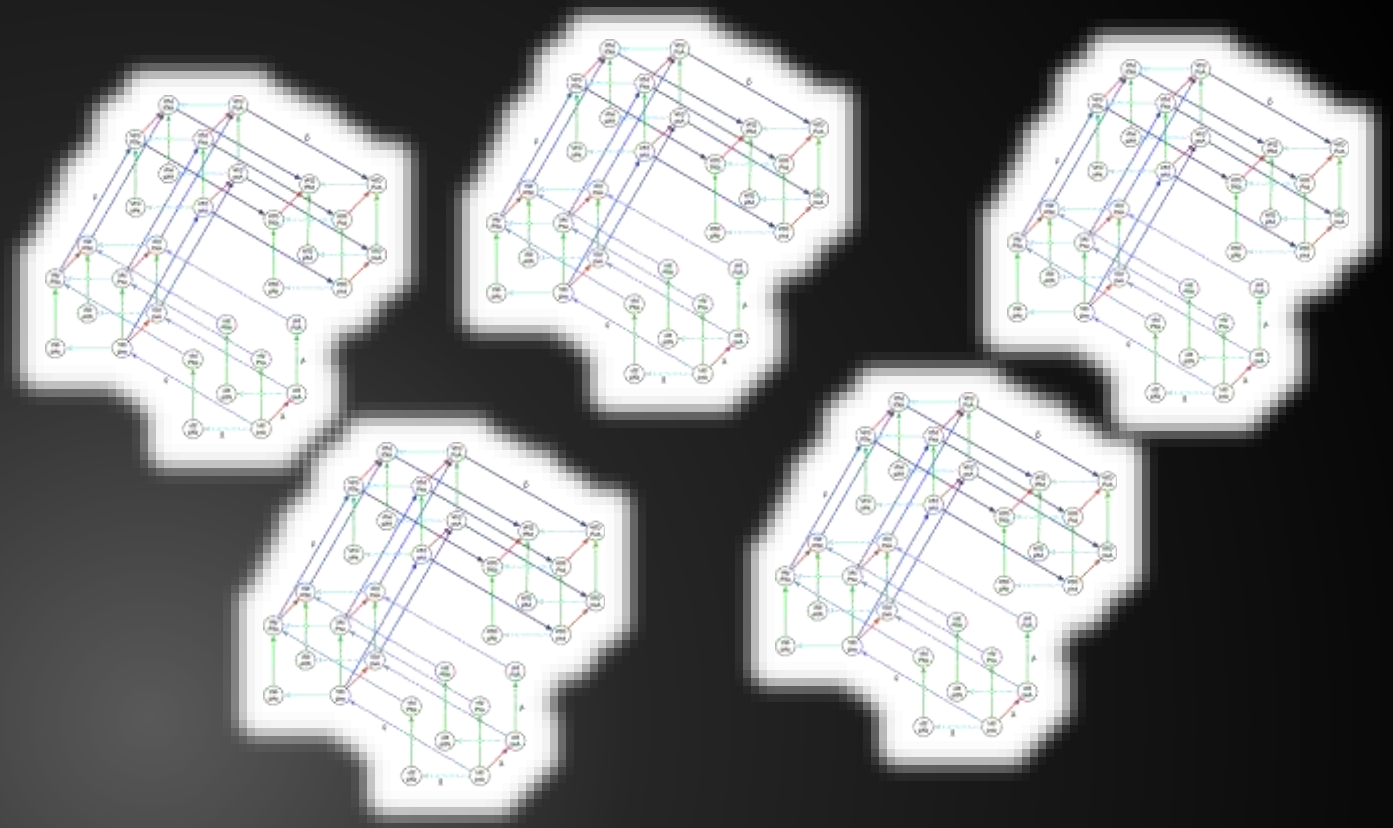
Measuring skill in CVD

Extending metrics to MPCVD

Applications

EACH VENDOR/PRODUCT

- is in its own state
- has its own history



SOME TRANSITIONS ARE SYNCHRONIZED, SOME ARE NOT

- Does publishing about a vul in A imply the vul is in B?
- Does an exploit for product A work on product B?

MPCVD GOALS

Avoid bad outcomes

avoid P, X, or A until everyone reaches F or even D

Achieve high ranked histories

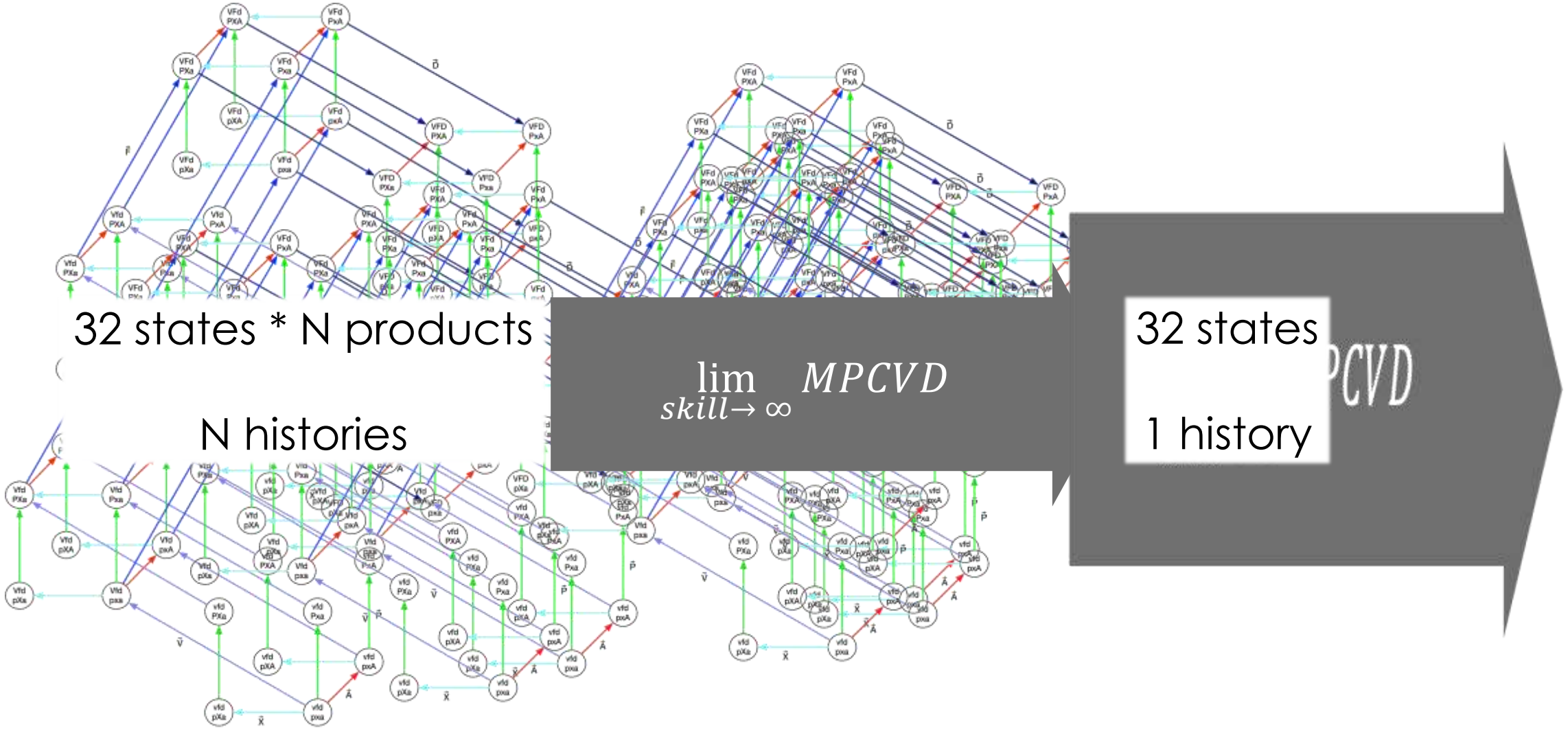
High median (accuracy)

Achieve consistent history ranks

Low entropy (precision)

Synchronize some transitions (e.g., F, P, even D)

MPCVD REDUCES CASE STATE ENTROPY

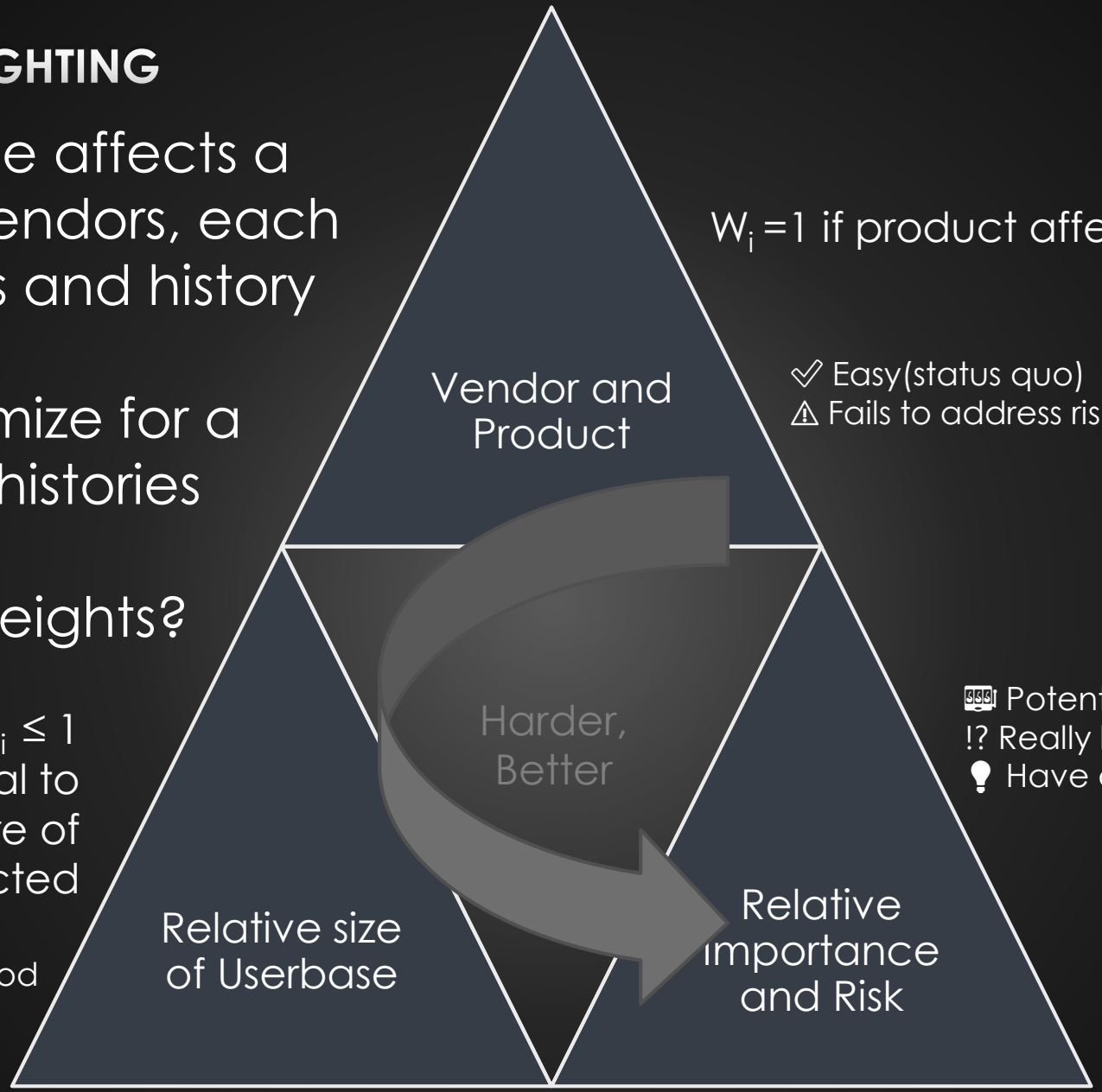


MPCVD HISTORY WEIGHTING

Each MPCVD case affects a set of products/vendors, each with its own states and history

MPCVD can optimize for a weighted sum of histories

What to use for weights?



W_i =1 if product affected, otherwise 0

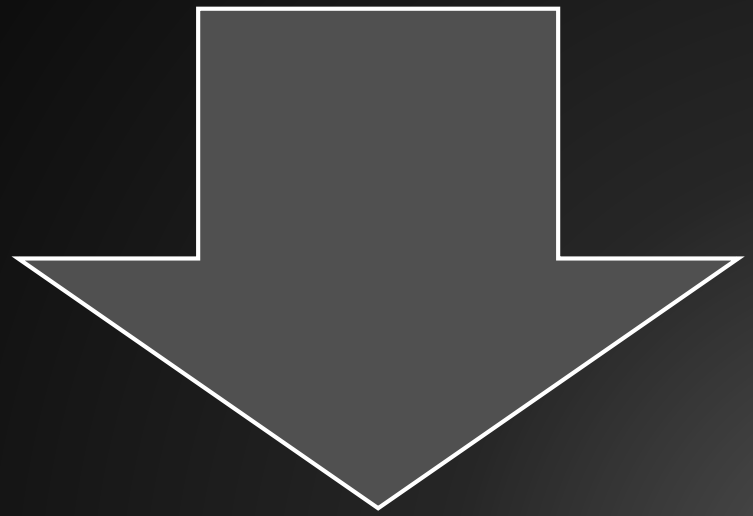
✓ Easy(status quo)
⚠ Fails to address risk diversity

$0 \le W_i \le 1$ proportional to market share of product affected

♻ Closer to aggregate social good
? Harder to measure
🏢 Favors larger products
☄ Still falls short on risk diversity

Potential to address high-risk niche usage
!? Really hard to measure
💡 Have a special "high risk" flag?

$0 \le W_i \le 1$ proportional to risk share of product affected



embargo duration

Faster, Stronger

embargo size

AGENDA

But how does this any of this help me?

Possible Histories of CVD

Structure of CVD states

Measuring skill in CVD

Extending metrics to MPCVD

Applications

APPLICATIONS

CLARIFY CVD ROLES
WHO CAN DO WHAT?

EMBARGO PATTERNS
WHERE DO EMBARGOES FIT?

CVD SITUATION AWARENESS
WHAT DO YOU KNOW?

CVD ACTION PROMPTS
WHAT CAN YOU DO?

POLICY FORMALISMS
WHAT CAN OTHERS EXPECT YOU TO DO?

DEFINING STICKY TERMS
WHAT DO YOU REALLY MEAN TO SAY?

NAVIGATING CVD
WHERE DO WE GO NOW?

CVD STATES
PUTTING IT ALL TOGETHER

CLARIFY CVD ROLES

WHO CAN DO WHAT?

CVD ROLES AND THE TRANSITIONS THEY CAN INDUCE

V	Vendor	Finder / Reporter	Deployer	Coordinator	Adversary
F	Vendor	Finder / Reporter	Deployer	Coordinator	Adversary
D	Vendor	Finder / Reporter	Deployer	Coordinator	Adversary
P	Vendor	Finder / Reporter	Deployer	Coordinator	Adversary
X	Vendor	Finder / Reporter	Deployer	Coordinator	Adversary
A	Vendor	Finder / Reporter	Deployer	Coordinator	Adversary

Role combinations are possible:

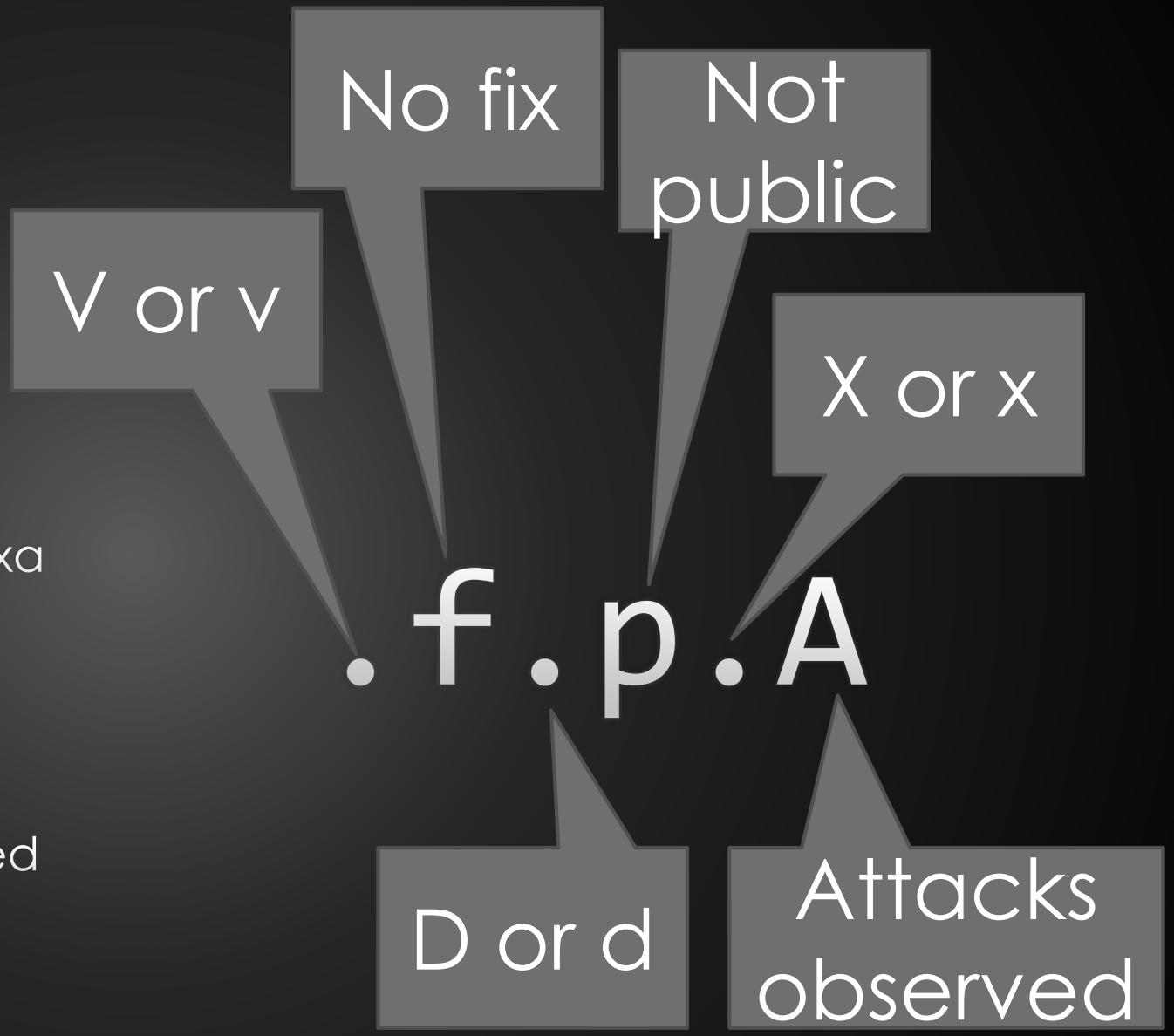
- Vendor + Finder/Reporter
- Vendor + Deployer
- Finder/Reporter + Adversary
- Etc.

EMBARGO PATTERNS

WHERE DO EMBARGOES FIT?

NOTATION

- All patterns assume order: vfdpxa
- Dots are wildcards
- Lowercase = event has not occurred
- Uppercase = event has occurred



WHEN CAN YOU START AN EMBARGO?

Why start an embargo if the fix is already deployed?

. . . d . . .

WHEN CAN YOU START AN EMBARGO?

Why start an embargo if the fix is already deployed?

If vul is public, what purpose does the embargo serve?

. . dp . .

WHEN CAN YOU START AN EMBARGO?

Why start an embargo if the fix is already deployed?

If vul is public, what purpose does the embargo serve?

If exploit is public, vul is or will soon be public.

. . dpx .

WHEN CAN YOU START AN EMBARGO?

Why start an embargo if the fix is already deployed?

If vul is public, what purpose does the embargo serve?

If exploit is public, vul is or will soon be public.

If attacks are happening, who is the embargo protecting?

. . dpxa

WHEN CAN YOU START AN EMBARGO?

Why start an embargo if the fix is already deployed?

If vul is public, what purpose does the embargo serve?

If exploit is public, vul is or will soon be public.

If attacks are happening, who is the embargo protecting?

. . dpxa

. fdpxa? (maybe)

WHEN SHOULD YOU *MAINTAIN* AN EMBARGO?

~~Why start an embargo if the fix is already deployed?~~

If vul is public, what purpose does the embargo serve?

If exploit is public, vul is or will soon be public.

If attacks are happening, who is the embargo protecting?

. . . pxa

Why keep embargo when the fix is already deployed?
E.g., web vul where site owner fixes but chooses to never disclose

MORE EMBARGO PATTERNS

Rule	States
Embargo can start	..dpxa
Embargo is viable	...pxa
Consider necessity of starting or continuing embargo	VFd...
Do not initiate new embargo existing embargo may continue (although value is questionable)	VFDpxa
Embargo is at risk	...p.A
Embargo is at imminent risk	...pX.
Embargo no longer viable	...P.. ....X. .....A

CVD SITUATION AWARENESS

WHAT DO YOU KNOW?

WHAT DO YOU KNOW AND WHEN?

WHAT YOU KNOW	STATE PATTERN
Attack success is likely	..d...
Attack success is unlikely	..D...
Expect vendor awareness imminently	v..P..
Expect both public and vendor awareness imminently	v..pX.
Expect public awareness imminently	V..pX.

WHAT DO YOU KNOW AND WHEN? (SSVC 2)

WHAT YOU KNOW	STATE PATTERN
SSVC contacted: No	v.....
SSVC public: No SSVC value added: precedence	...p..
SSVC public: Yes	...P..
SSVC exploitation: High	.....A
SSVC exploitation: Low	....xa
SSVC exploitation: Moderate	....Xa
SSVC value added: Ampliative	VF.p..
SSVC value added: Limited	VF.P..

WHAT DO YOU KNOW AND WHEN? (CVSS 3.1)

WHAT YOU KNOW	STATE PATTERN
CVSS 3.1 exploit maturity: H, F, or P	....Xa
CVSS 3.1 exploit maturity: H or F	....XA
CVSS 3.1 remediation level: X, U, W, or T	Vf....
CVSS 3.1 remediation level: T or O	VF....

WHAT DO YOU KNOW AND WHEN? (VEP)

WHAT YOU KNOW	STATE PATTERN
VEP remains tenable	vfdpx.
VEP does not apply	V.....
VEP does not apply	...P..
VEP does not apply	....X.
Adversarial utility remains viable	..d...

Note that `..d...` (24 states)
is much bigger than `vfdpx.` (2 states)

CVD ACTION PROMPTS

What can you do?

WHAT CAN YOU DO AND WHEN?

ACTION	EVENT TRIGGERED	STATE PATTERN
Notify vendor	V	v.....
Terminate existing embargo	-	...P..
Monitor for exploit publication	-	....x.
Monitor for exploit refinement Publish detection for exploits Terminate existing embargo	-	....X.
Monitor for attacks	-	.....a
Monitor for additional attacks Terminate any existing embargo	-	.....A
Monitor public reports	V	v..P..
Publish vul and any mitigations (if no active embargo)	P	V..p..

WHAT CAN YOU DO AND WHEN?

ACTION	EVENT TRIGGERED	STATE PATTERN
Draw attention to published exploits Publish mitigations Do nothing	P	`...pX.`
Draw attention to published exploits Publish mitigations	-	`...PX.`
Publish mitigations	P	`...p.A`
Escalate response priority among responding parties	-	`..d.X.` `..d..A`
Create fix (vendor) Encourage vendor to create fix (non-vendor)	F	`Vfd...`

Escalate response priority among responding parties	-	`.fdP..`
		`.fd.X.`
		`.fd..A`

WHAT CAN YOU DO AND WHEN?

ACTION	EVENT TRIGGERED	STATE PATTERN
Maintain any existing disclosure embargo Maintain vigilance for disclosure embargo exit criteria	-	...pxa
Publish vul and any mitigations (if no vendor exists)	P	vfdp..
Escalate fix priority with vendor	F	VfdP..
Escalate vigilance for exploit publication Escalate vigilance for attacks Publish mitigations	-	VfdP..
Publish vulnerability (motivate vendor to fix, motivate deployers to mitigate)	P	Vfdp..
Encourage vendor to deploy fix (if possible) Deploy fix (vendor)	D	VFdp..
Publish fix	P	VFdp..

WHAT CAN YOU DO AND WHEN?

ACTION	EVENT TRIGGERED	STATE PATTERN
Deploy fix (deployer) Promote fix deployment (non-deployer)	D	VFdP..
Publish vul (for future reference)	P	VFDp..
Discourage exploit publication until F	-	.fd.xa
Publish mitigations (if possible) Terminate embargo and publish early	P	.fdpX. .fdp.A
Negotiate or establish disclosure embargo	-	..dpxa
Prepare to break existing embargo	-	Vf.pX. Vf.p.A
Encourage/cause publication of exploit code (promote defense/detection)	X	.f.PxA

WHAT CAN YOU DO AND WHEN?

ACTION	EVENT TRIGGERED	STATE PATTERN
Initiate VEP	-	vfdpx.
Consider appropriateness of initiating a new embargo	-	VFdpxa
Encourage/cause publication of exploit code (promote deployment, detection)	X	VFdPxa
Close case	-	VFDPXA
Close case (unless monitoring for X or A)	-	VFDPxa VFDPXa VFDPxA

POLICY FORMALISMS

WHAT CAN OTHERS EXPECT YOU TO DO?

TRANSLATING GPZ POLICY 2021

Policy Statement	(begin state, timer, end state)
Disclosure deadline of 90 days. If an issue remains unpatched after 90 days, technical details are published immediately.	(Vfdpxa, 90, VfdPxa)
If the issue is fixed within 90 days, technical details are published 30 days after the fix.	If (Vfdpxa, <=90, VF..xa) Then (VF..xa, 30, VF.Pxa)
A 14-day grace period* is allowed.	If (Vfdpxa, <90, Vfdpxa) + req Then (Vfdpxa,104,V..Pxa)
For issues that are being actively exploited in-the-wild against users...if an issue remains unpatched after 7 days, technical details are published immediately.	(Vfdp.A, 7, VfdP.A) (VfdpX., 7, Vf.PX.) (?)
If the issue is fixed within 7 days, technical details are published 30 days after the fix.	If (Vfdp.A, <=7, VF.p.A) Then (VF.p.A, 30, VF.P.A)
Vendors can request a 3-day grace period* for in-the-wild bugs.	If (Vfdp.A, <7, Vfdp.A) + req Then (Vfdp.A, 10, V.dP.A)
Earlier disclosure with mutual agreement.	If req Then (V..pxa, <90, V..Pxa) Or (V..pxA, <7, V..PxA)

TRANSLATING CERT/CC POLICY 2021

Policy Statement	(begin state, timer, end state)
Vulnerabilities reported to the CERT/CC will be disclosed to the public 45 days after the initial report, regardless of the existence or availability of patches or workarounds from affected vendors.	...pxa, 45, ...Pxa
Extenuating circumstances, such as active exploitation, threats of an especially serious (or trivial) nature, or situations that require changes to an established standard may result in earlier or later disclosure.	...pX., <45, ...PX. ...p.A, <45, ...P.A If (extenuating circumstances) Then ...pxa, >45, ...Pxa
Vulnerabilities reported to us will be forwarded to the affected vendors as soon as practical after we receive the report.	v....., ASAP, V.....

This isn't a perfect way to specify policies.

But it might help us to move towards formalization of policies.

Potential benefits include:

- Recognizing and reasoning about gaps in existing policies
- Automated resolution of disclosure schedules based on solving policy logic

DEFINING STICKY TERMS

WHAT DO YOU REALLY MEAN TO SAY?

FORMALIZING DEFINITIONS: WHAT DO YOU MEAN, "ZERO DAY"?

#	What kind of 0-day?	Words	State Pattern
1	Vulnerability	...unknown to the vendor, exploitable, and not publicly known. (VEP)	v..p..
2	Vulnerability	...public before the vendor is aware	v..P..
3	Vulnerability	...public before a fix is available	.f.P..
4	Exploit	...released before vendor is aware	v...X.
5	Exploit	...released before fix is available	.f..X.
6	Exploit	...released before public is aware	...pX.
7	Attack	...occurs before vendor aware	v....A
8	Attack	...occurs before fix is available	.f...A
9	Attack	...occurs before public is aware	...p.A

https://insights.sei.cmu.edu/blog/like-nailing-jelly-to-the-wall-difficulties-in-defining-zero-day-exploit/

FORMALIZING DEFINITIONS: FOREVER DAY VULNERABILITY

#	Words	State Pattern
1	Vendor has designated product as end-of-life (EoL)	Vf....
2	Vendor no longer exists	vf....
3	Deployer chooses not to deploy	..d...

https://insights.sei.cmu.edu/blog/like-nailing-jelly-to-the-wall-difficulties-in-defining-zero-day-exploit/

NAVIGATING CVD

WHERE DO WE GO NOW?

NAVIGATION STRATEGY

LEGEND
New lock-in win
Inherited win
Available future
Locked-in loss

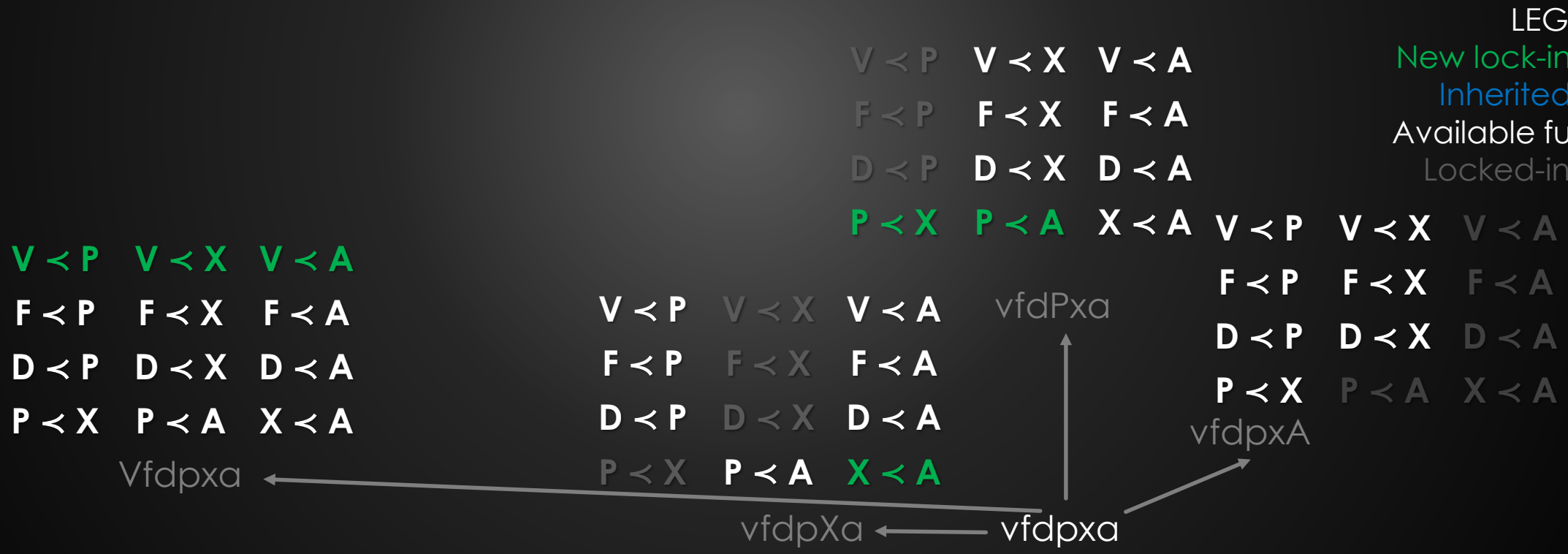
1. Chose next node with most total wins
2. If tied, choose next node with most available futures
3. If still tied, choose randomly

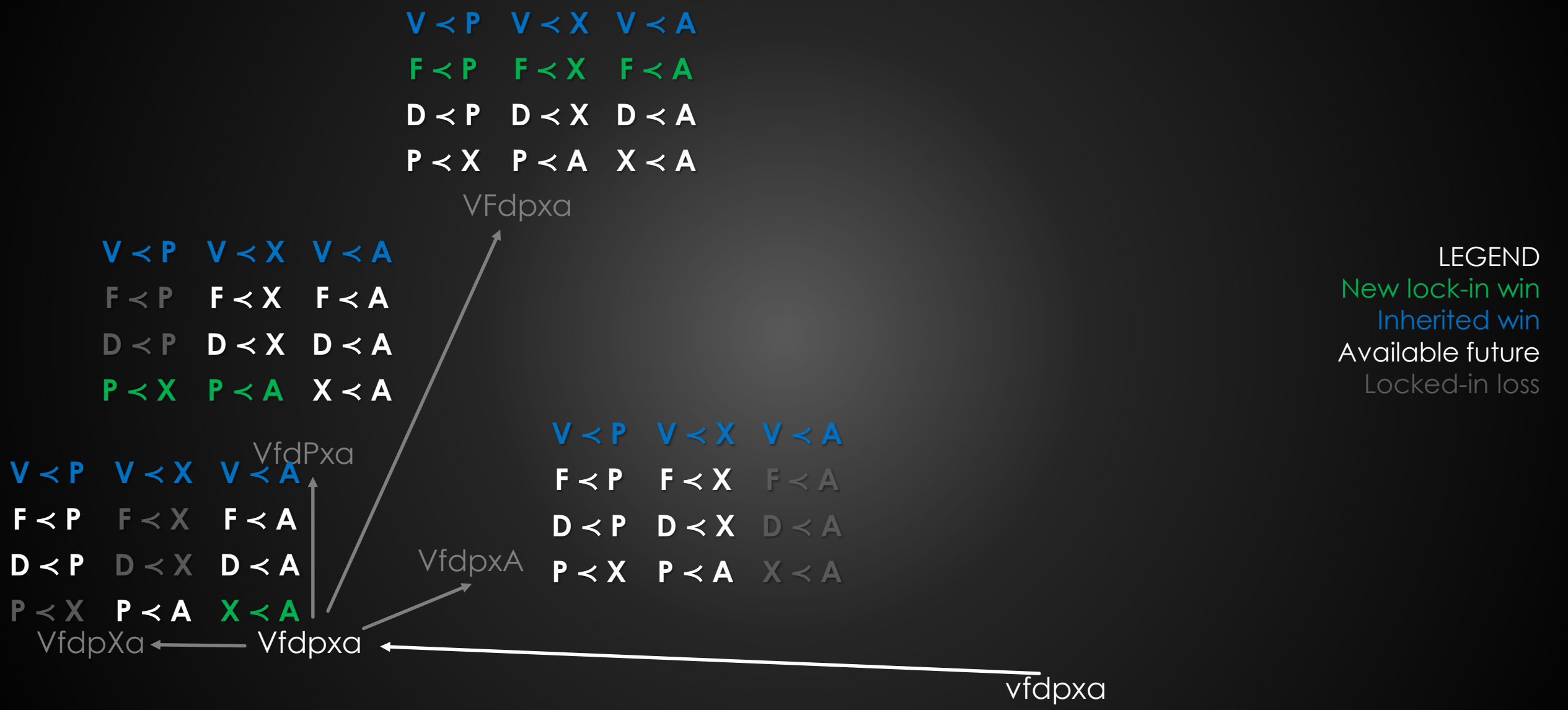
$V \prec P \quad V \prec X \quad V \prec A$

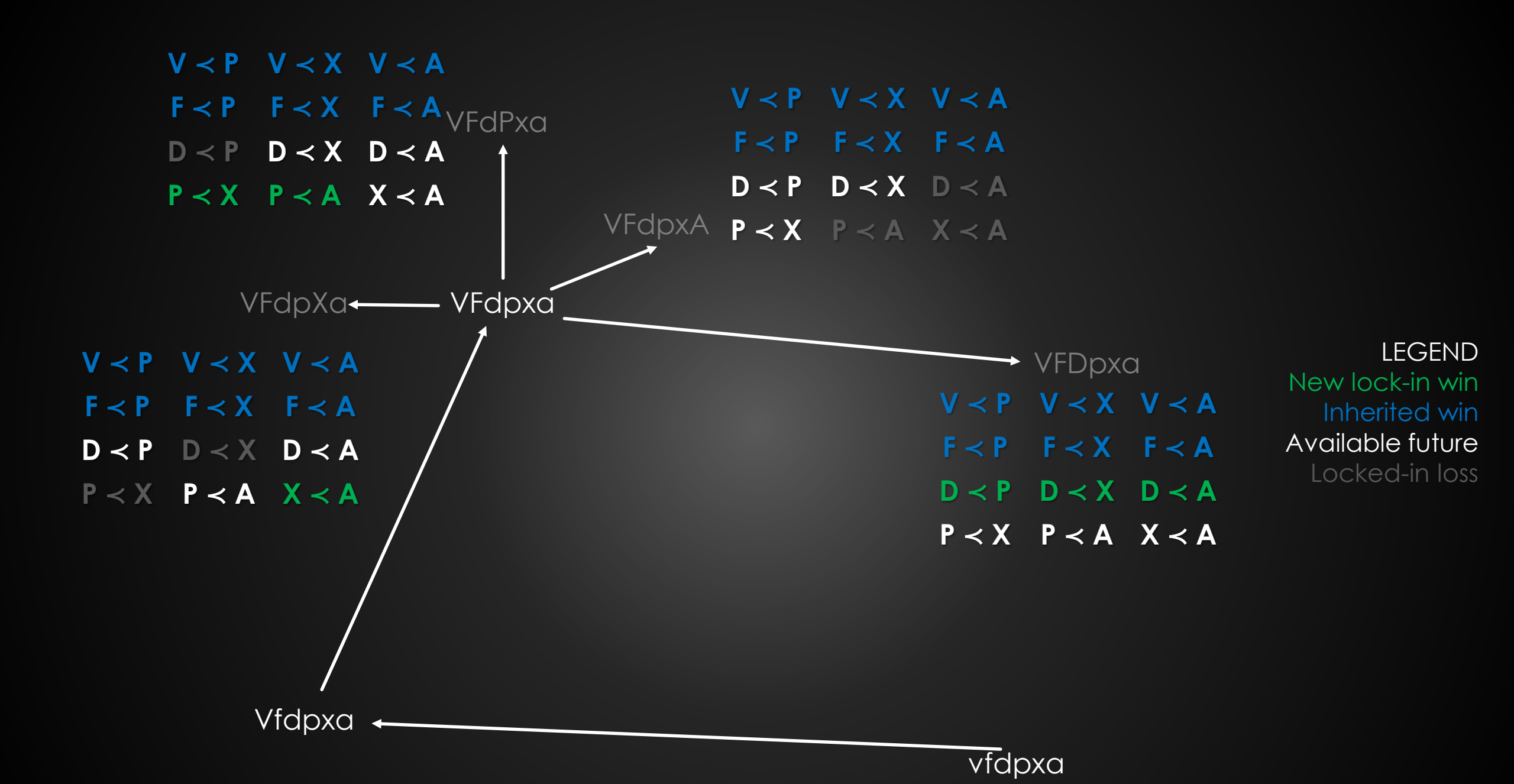
$F \prec P \quad F \prec X \quad F \prec A$

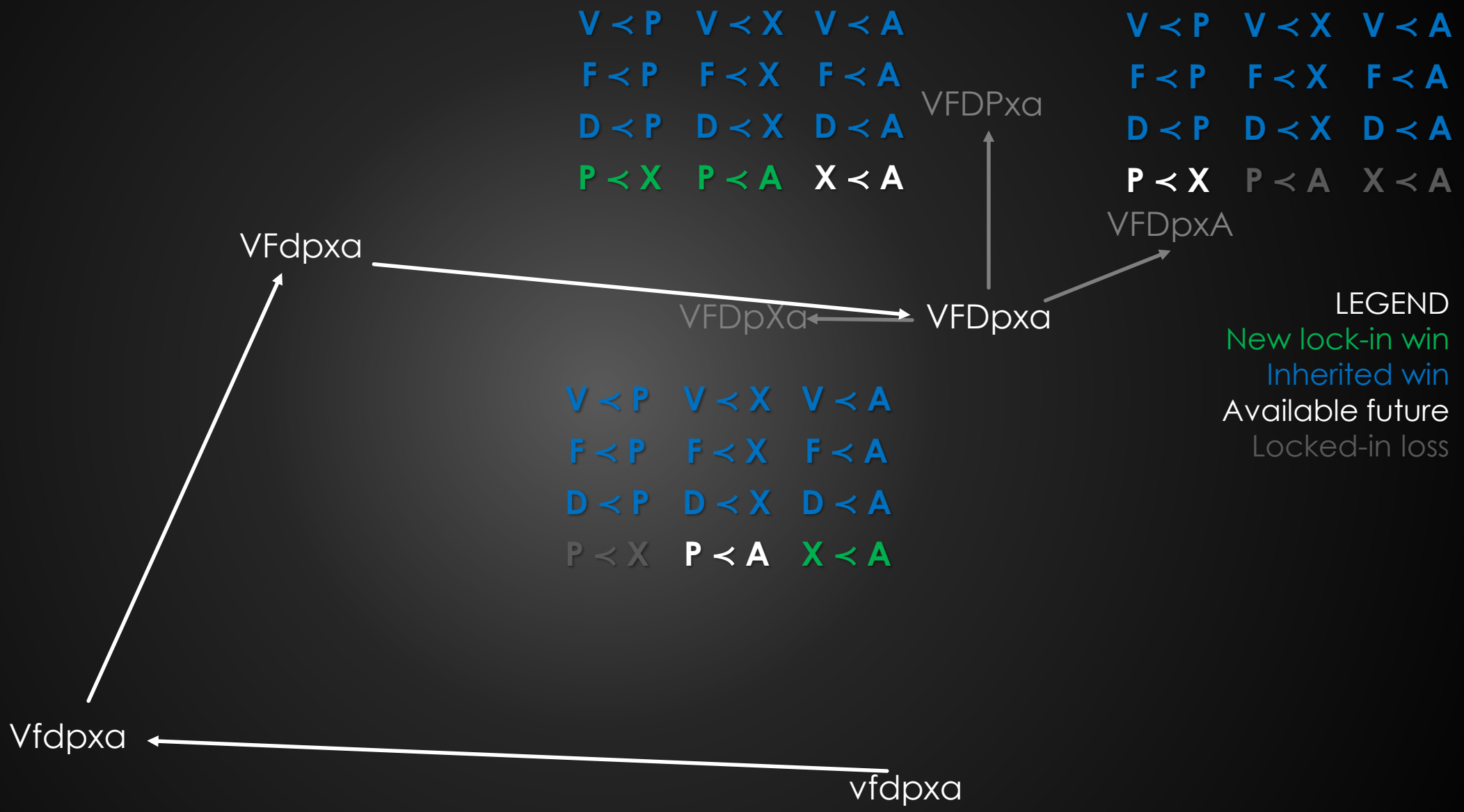
$D \prec P \quad D \prec X \quad D \prec A$

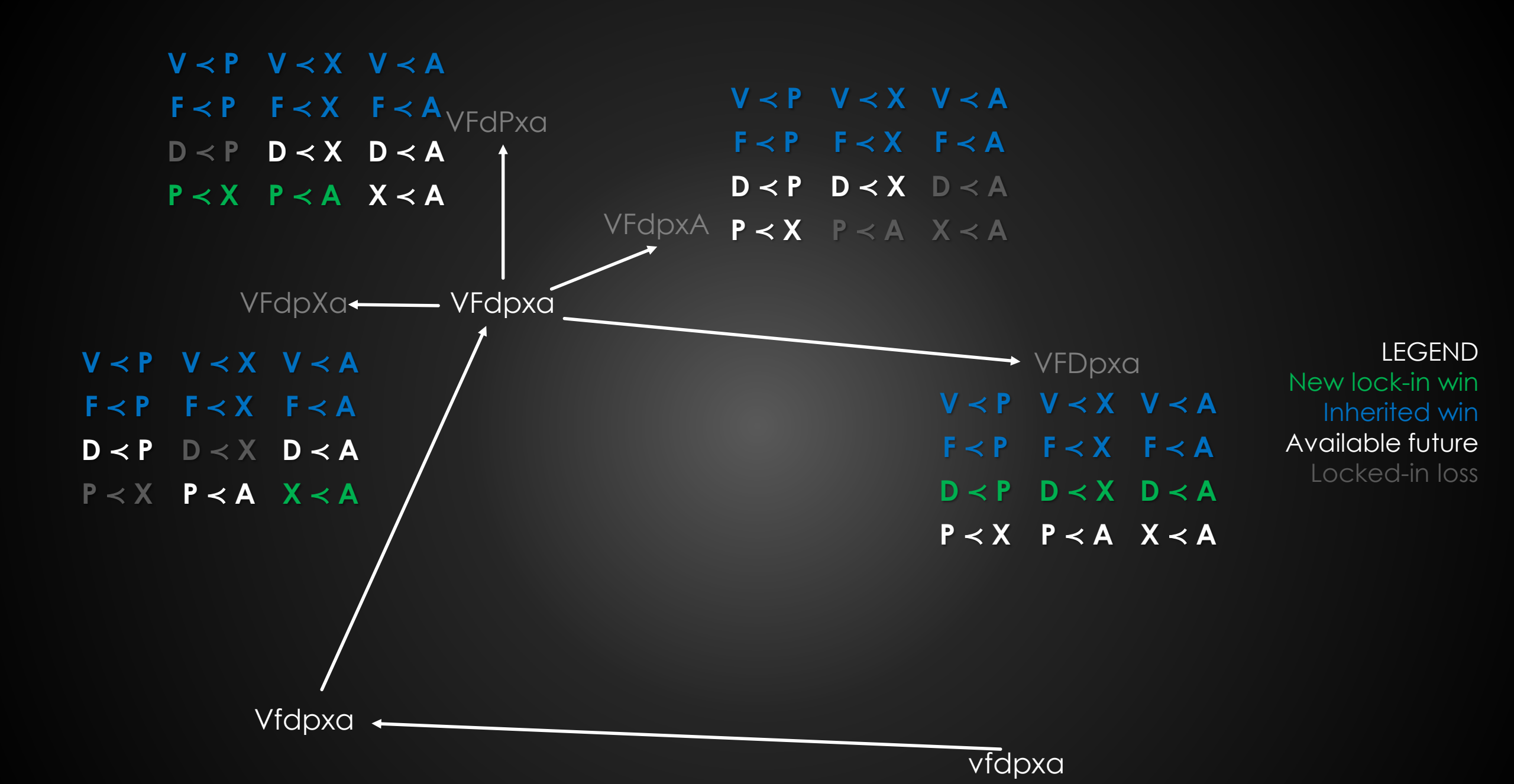
$P \prec X \quad P \prec A \quad X \prec A$

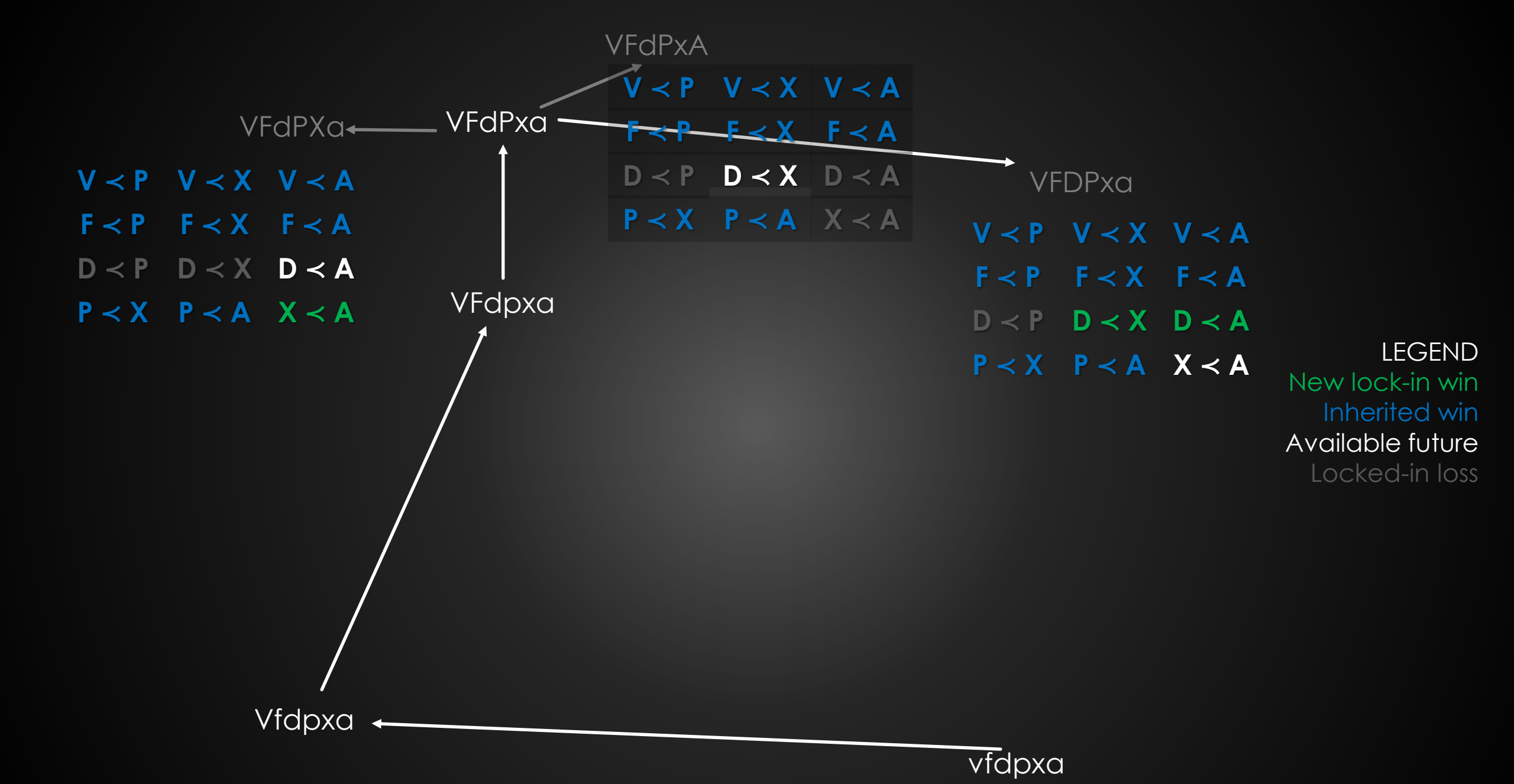


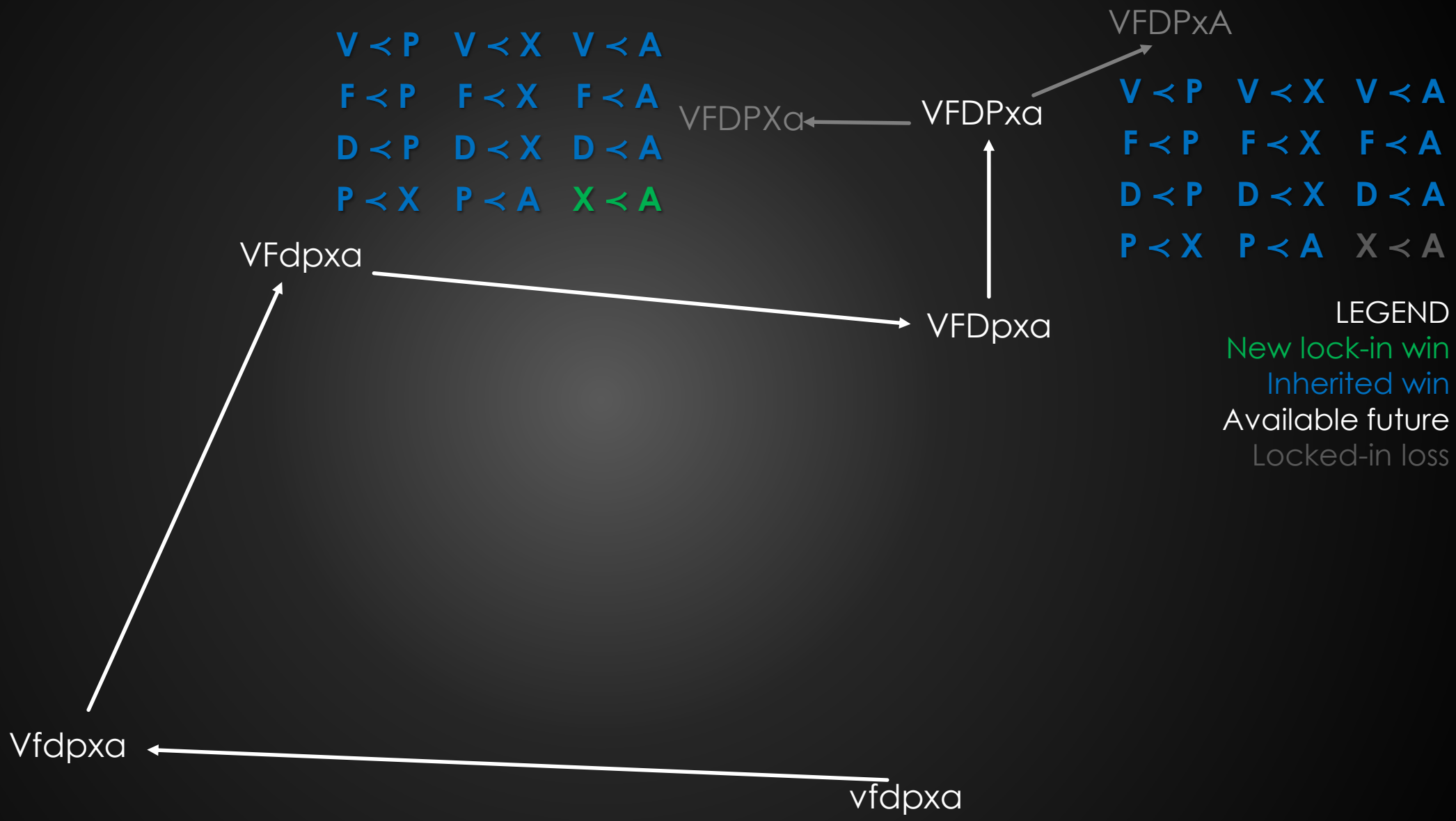










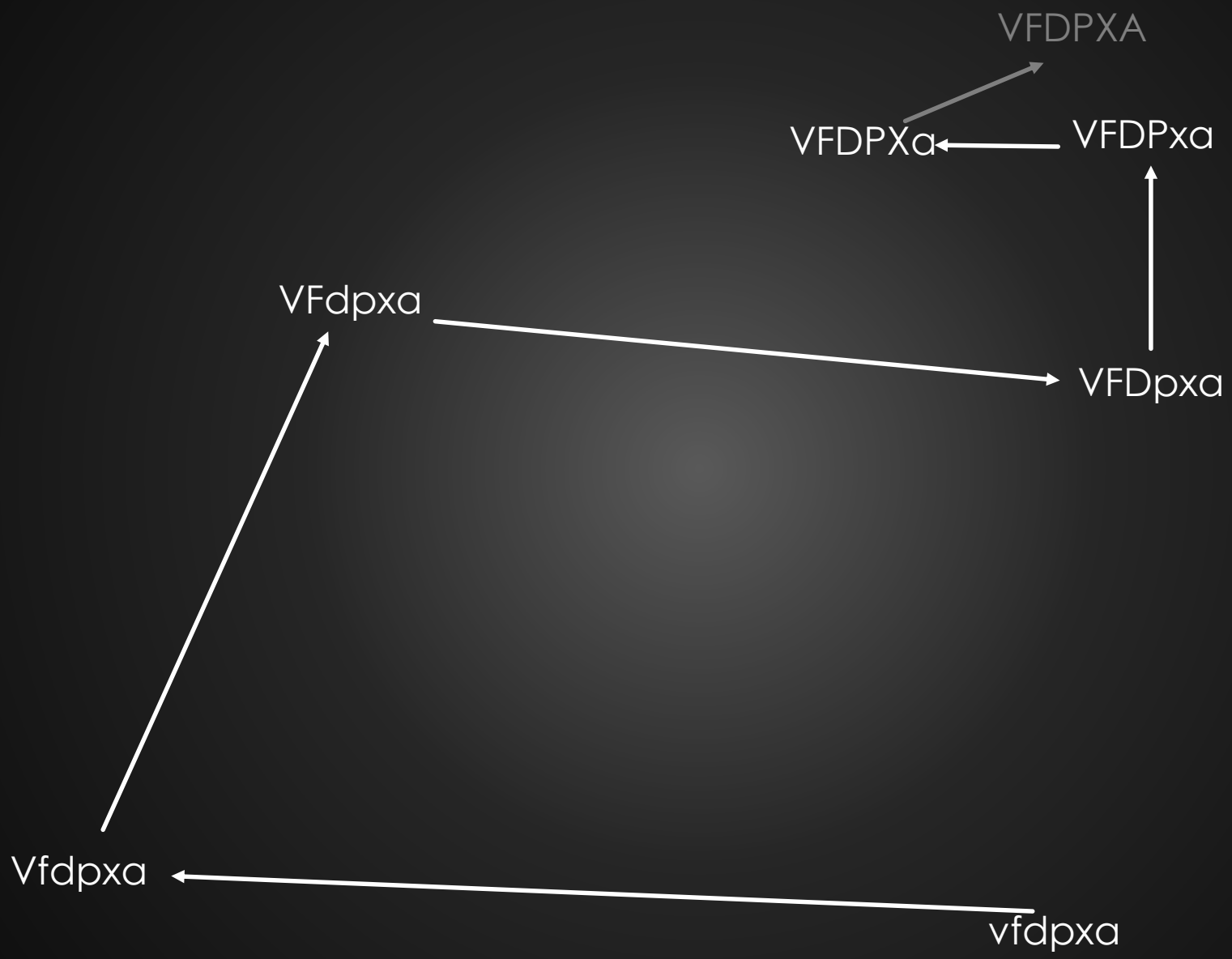


$V \prec P$ $V \prec X$ $V \prec A$

$F \prec P$ $F \prec X$ $F \prec A$

$D \prec P$ $D \prec X$ $D \prec A$

$P \prec X$ $P \prec A$ $X \prec A$



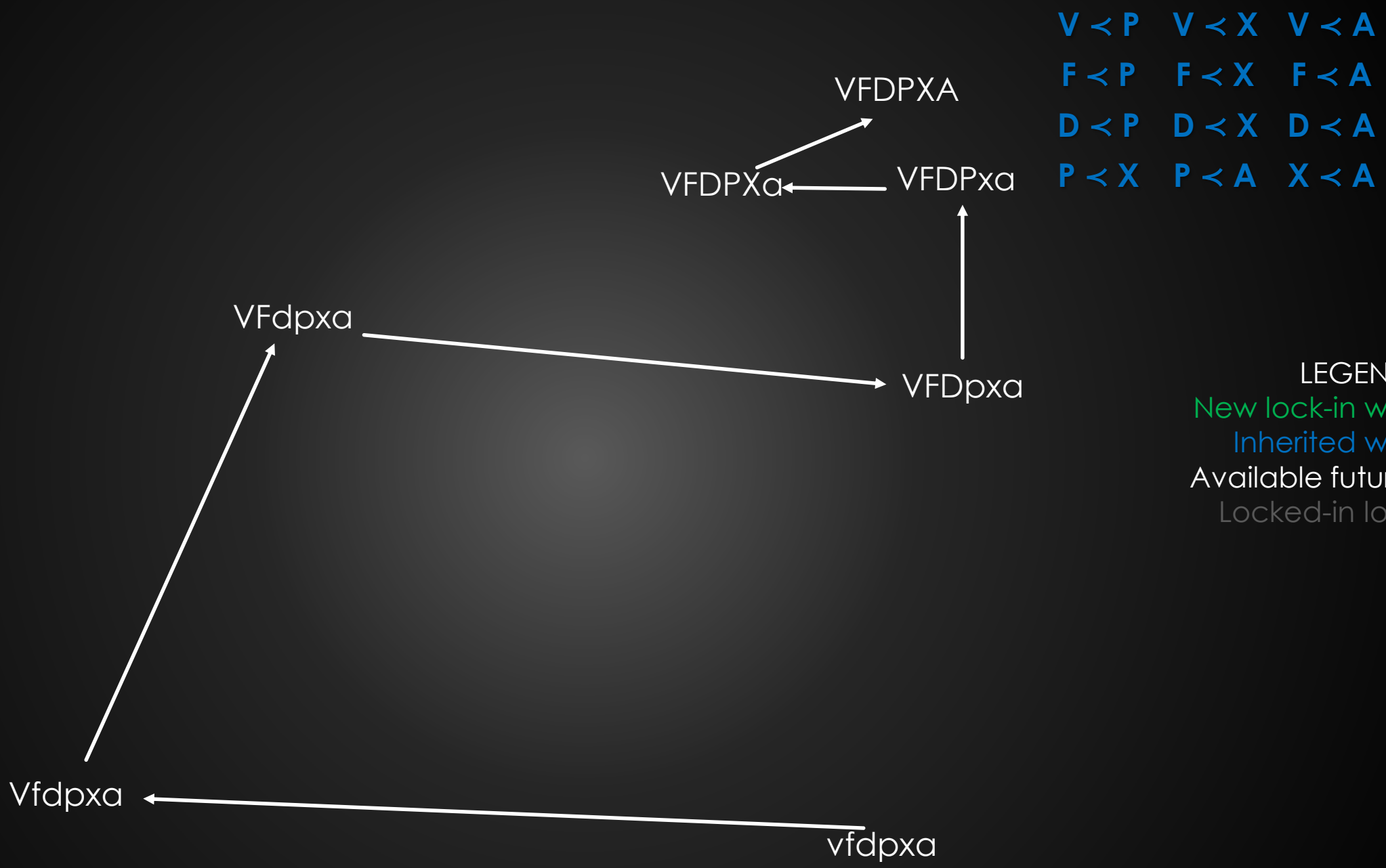
LEGEND

New lock-in win

Inherited win

Available future

Locked-in loss



$V \prec P$ $V \prec X$ $V \prec A$
$F \prec P$ $F \prec X$ $F \prec A$
$D \prec P$ $D \prec X$ $D \prec A$
$P \prec X$ $P \prec A$ $X \prec A$

LEGEND
New lock-in win
Inherited win
Available future
Locked-in loss

CVD STATES

PUTTING IT ALL TOGETHER

vfd...

Vfd...

VFd...

VFD...

vfdpxa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

Next V F D P X A

actions

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

vfdpxA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

Next V F D P X A

actions

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

vfdpXa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

Next V F D P X A

actions

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

vfdpXA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

Next V F D P X A

actions

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

vfdPxa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

vfdPxA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

Next V F D P X A

actions

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

vfdPXa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

Next V F D P X A

actions

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

vfdPXA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

Vfdpxa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VfdpxA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

Next V F D P X A

actions

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VfdpXa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VfdpXA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VfdPxa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VfdPxA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

Next V F D P X A

actions

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VfdPXa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VfdPXA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFdpxa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFdpxA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFdpXa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFdpXA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFdPxa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFdPxA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFdPXa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFdPXA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFDpxa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFDpxA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFDpXa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFDpXA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFDPxa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFDPxA

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFDPXa

Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	

VFDPXA

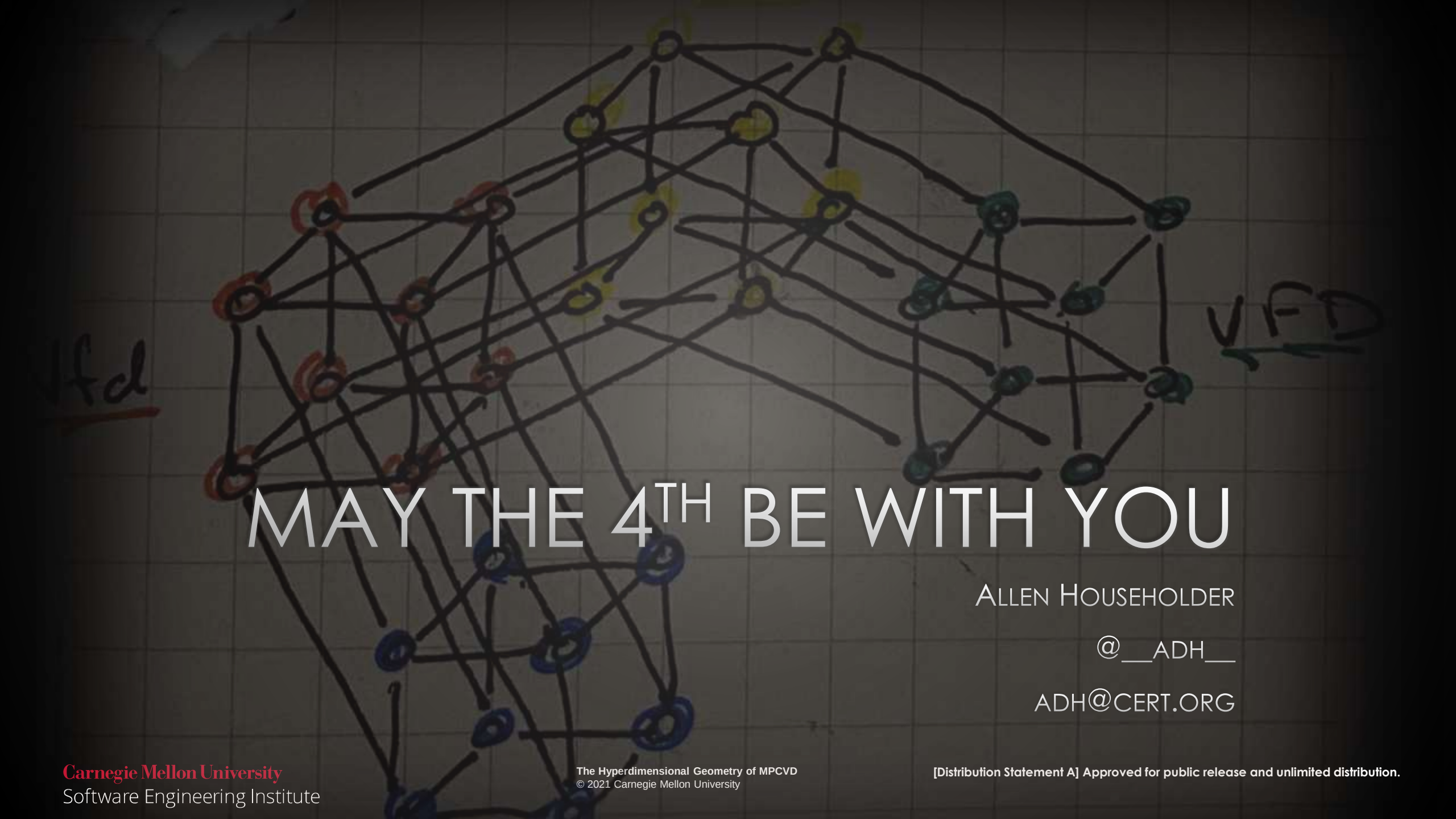
Vendor	is	is not	aware
Fix	is	is not	ready
Fix	is	is not	deployed
Public	is	is not	aware
Exploit	is	is not	public
Attacks	are	are not	observed

SSVC			
Contacted	No	Yes	
Exploitation	Low	PoC	Active
Public	No	Yes	
Value Added	Limited	Ampliative	Precedence
Supplier involvement	Unco-op.	Co-op.	Fix ready

actions

Next V F D P X A

Notify vendor [V]	Create fix (vendor) [F]	Deploy fix (vendor) [D]	Deploy fix (!vendor) [D]	Close case
Publish mitigations [P]	Publish vulnerability [P]	Publish fix [P]	Publish exploit [X]	Publish detection [P]
Monitor for publication	Monitor for exploit	Monitor for attacks	↑ exploit vigilance	↑ attack vigilance
↑ notify priority	↑ fix priority	↑ deploy priority	↑ publish priority	
Initiate embargo	Maintain embargo	Prepare embargo exit	Terminate embargo	Avoid embargo
Enc. Vendor create fix	Enc. Vendor pub fix	Enc. Vendor deploy fix	Enc. Deployer deploy fix	



MAY THE 4TH BE WITH YOU

ALLEN HOUSEHOLDER

@__ADH__

ADH@CERT.ORG

Carnegie Mellon University
Software Engineering Institute