Extending Anticipation Games with Location, Penalty and Timeline

Elie Bursztein
LSV, ENS-Cachan

I. Background
II. Location
III. Timeline
IV. Penalty

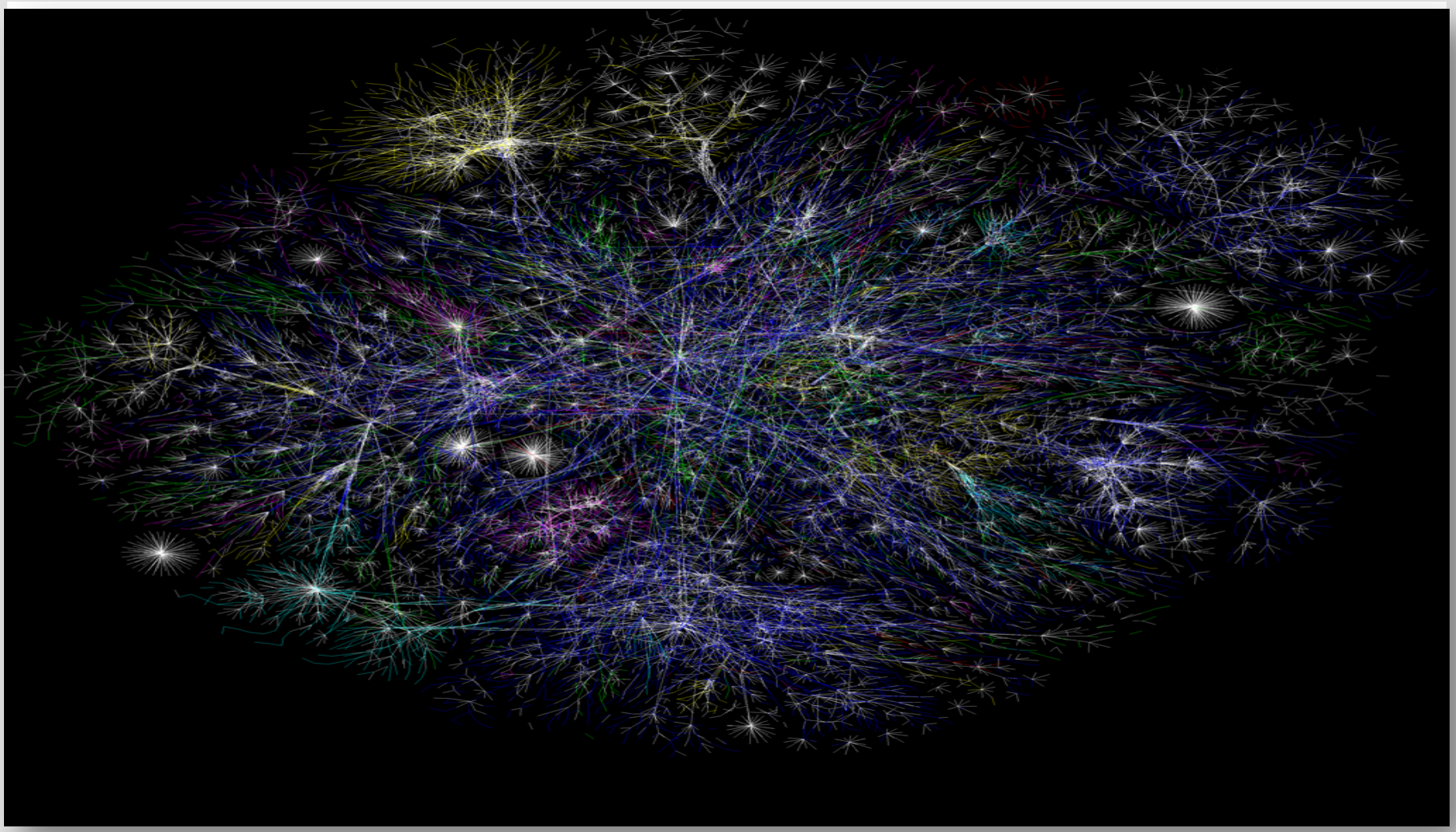
I. Background
II. Framework
III. Location
IV. Timeline
V. Penalty

Background

The art of war is of vital importance to the State.

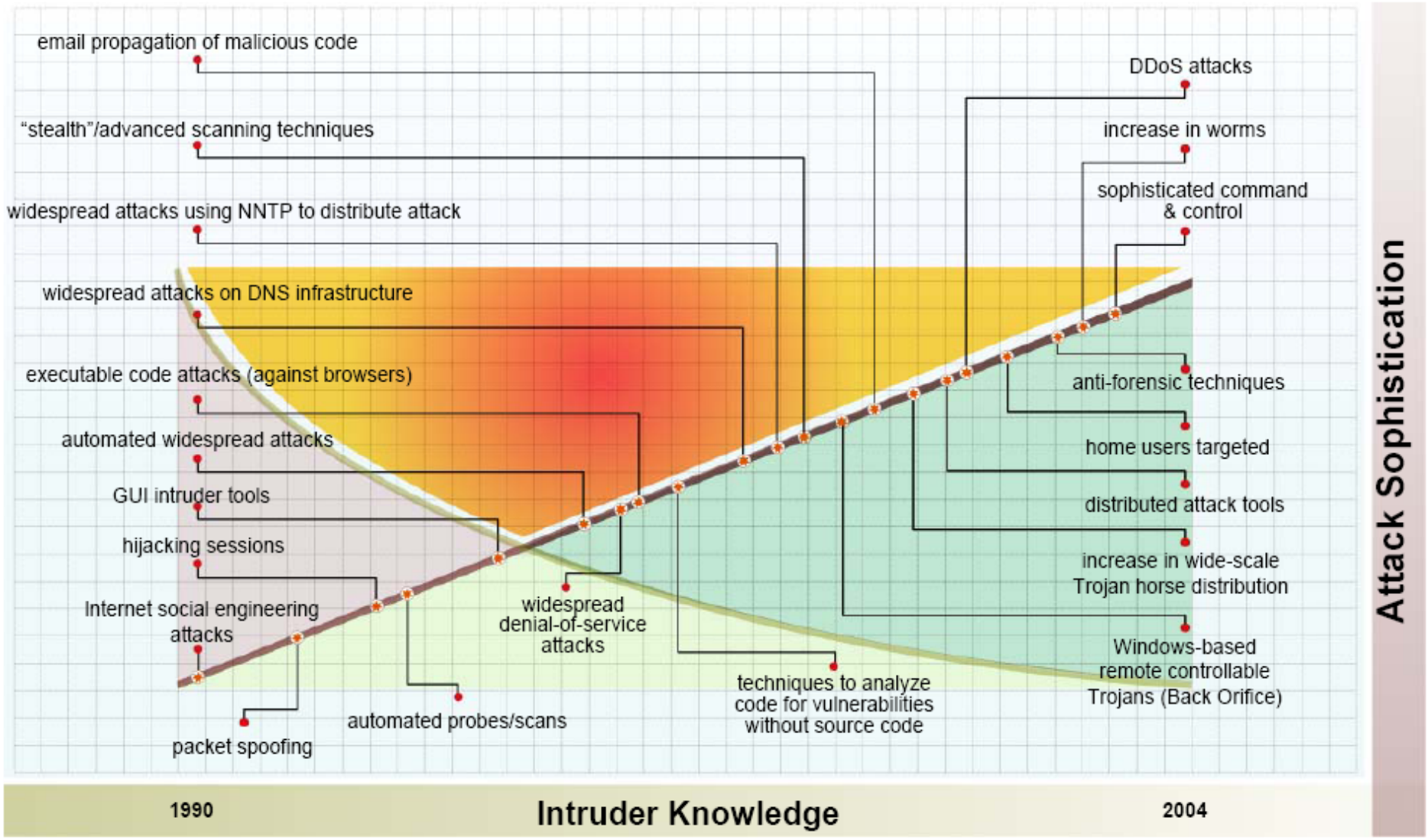
Sun Tzu, The art of war I.1

Network is getting more and more complex

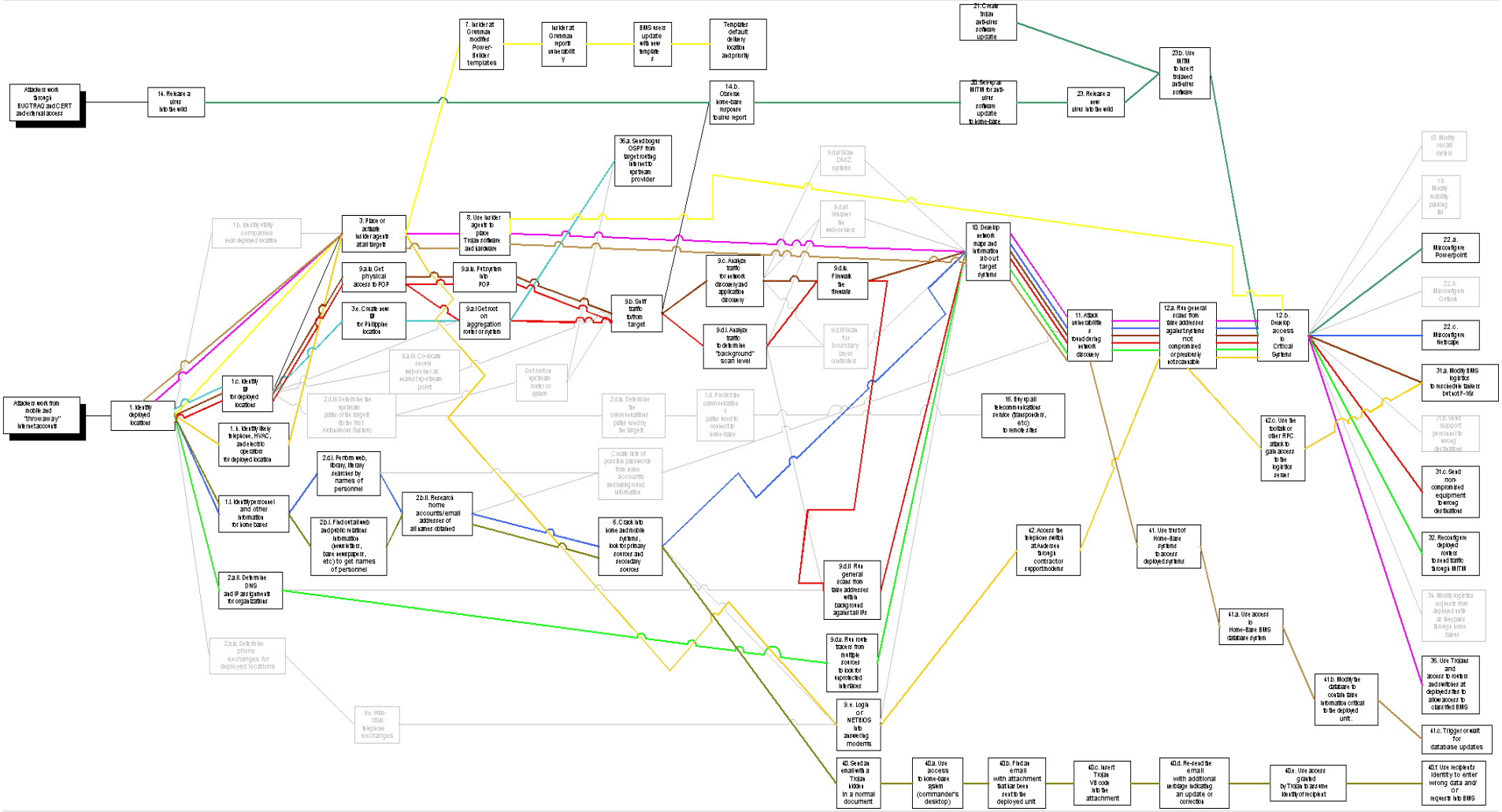


Opte project

Attack techniques are getting more and more sophisticated

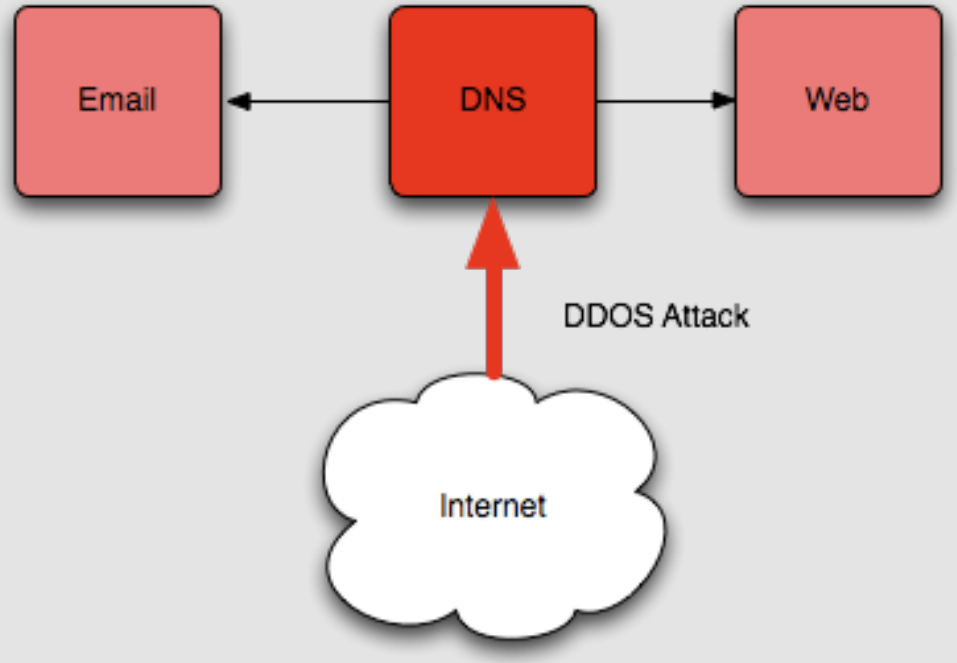


Cert/ Carnegie Mellon University



Sandia Red Team "White Board" attack graph from DARPA CC20008 Information battle space preparation experiment

Take into account the collateral damages



Exploit vulnerabilities

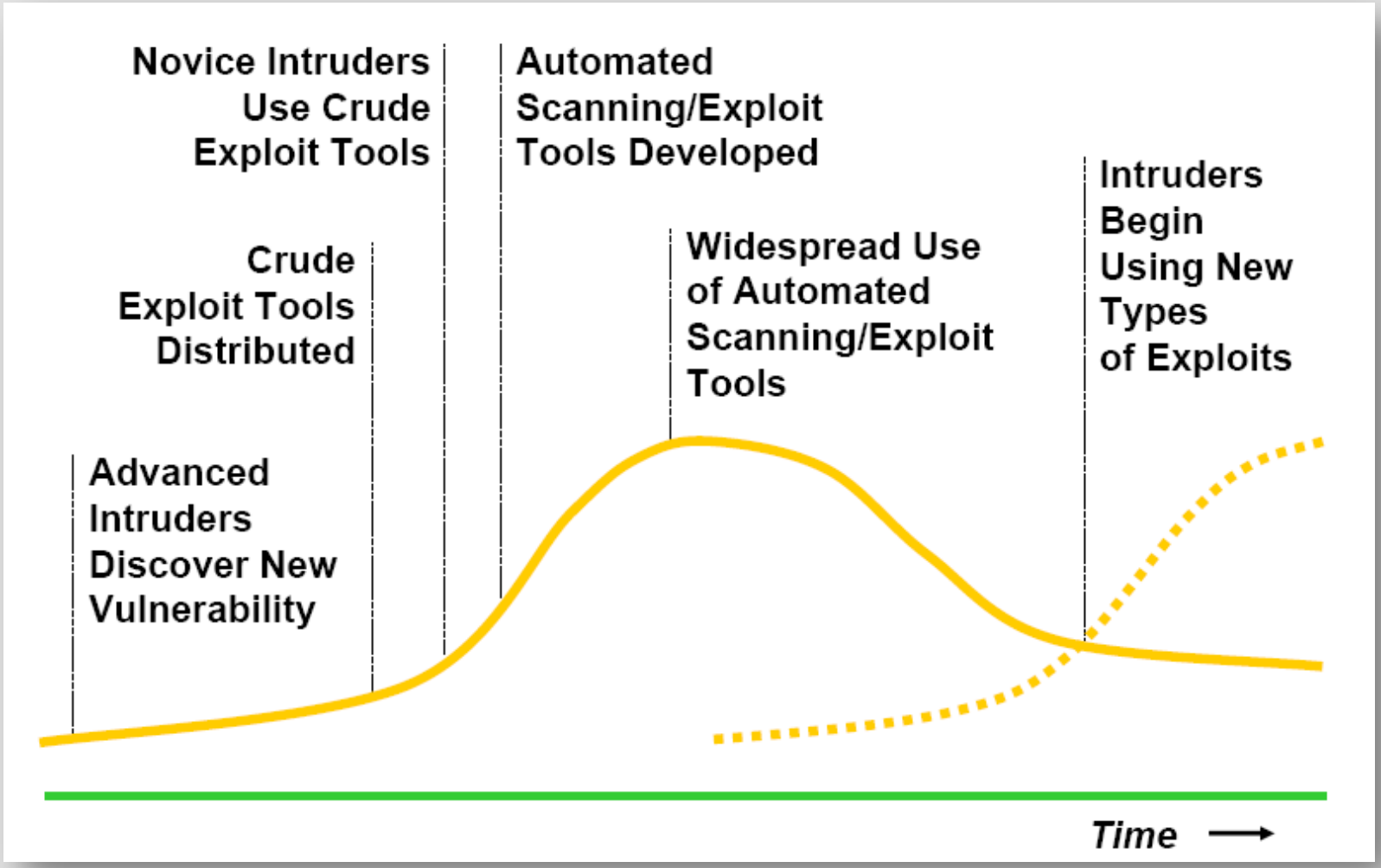
Abuse trust relations

Deal with the interaction of users

Patch

Firewall

Restore



Cert/ Carnegie Mellon University

Take into account the financial dimension

Network are very big so usual techniques does not work well

I. Background
II. Framework
III. Location
IV. Timeline
V. Penalty

Framework

In war, then, let your great object be victory, not lengthy campaigns.

Sun Tzu, The art of war II.19

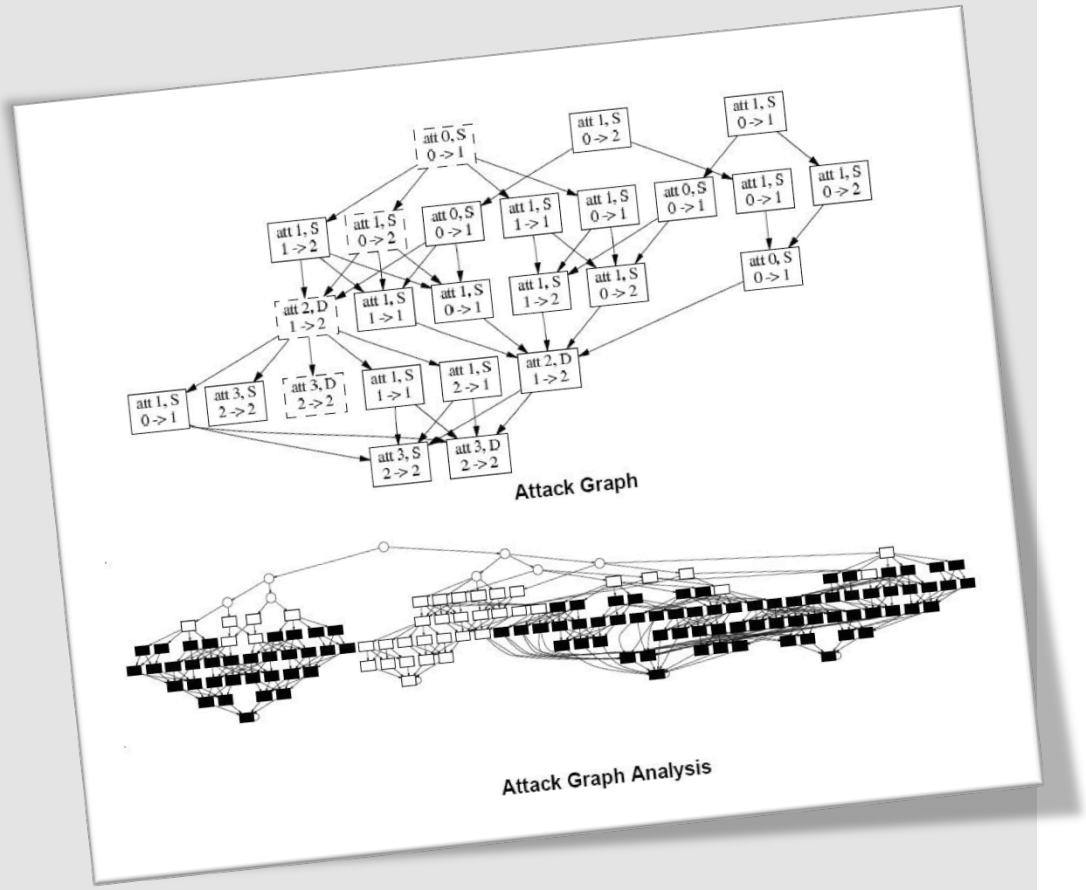
NetQi is a framework for network risk analysis

its a 4th generation* framework

*Baskerville classification 1993

Previous framework

- Attack graph
- NetSpa
- MulVal
- Cauldron



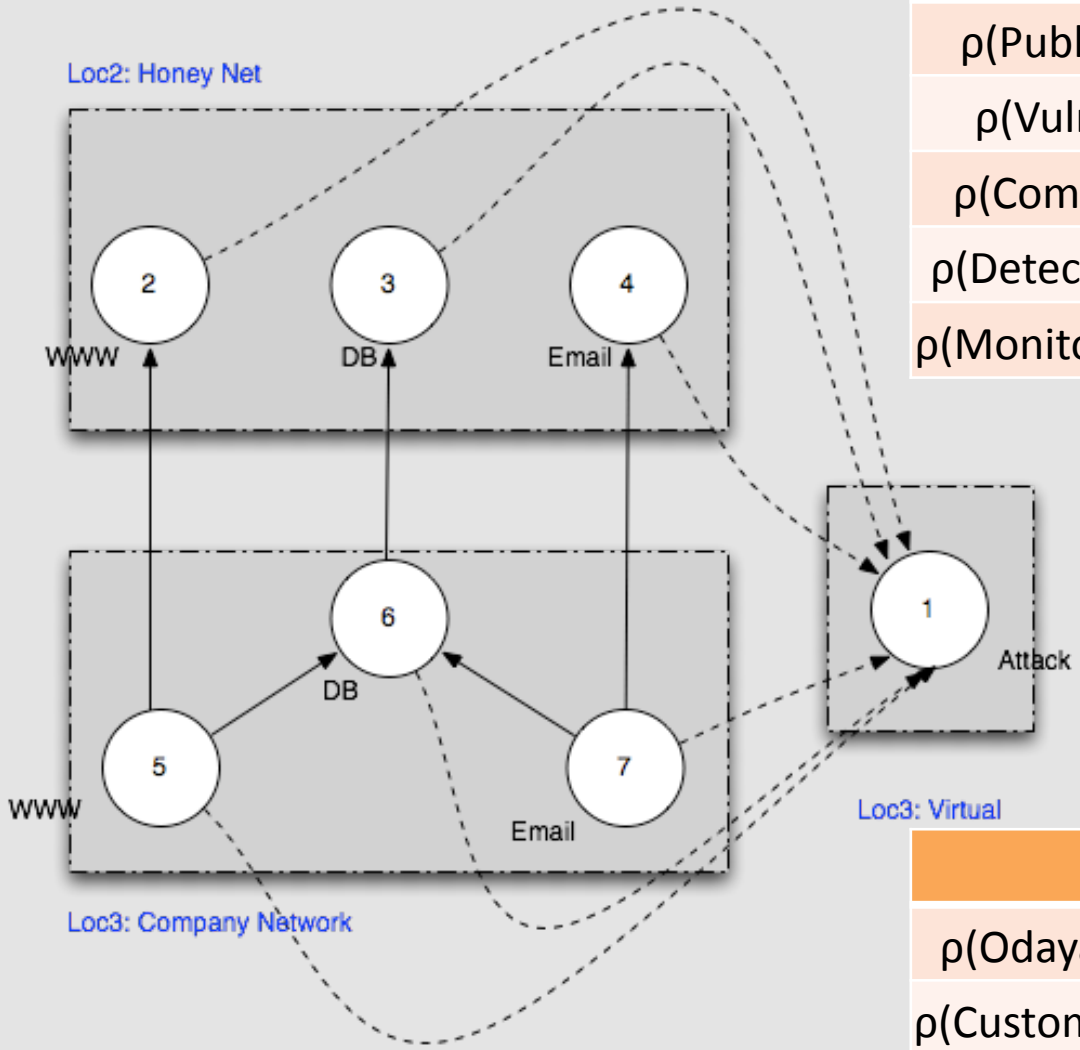
SEIR model

its model is based on game theory and modal logic

An anticipation game is a dual layer structure

The lower layer called dependency graph is used to represent the network state

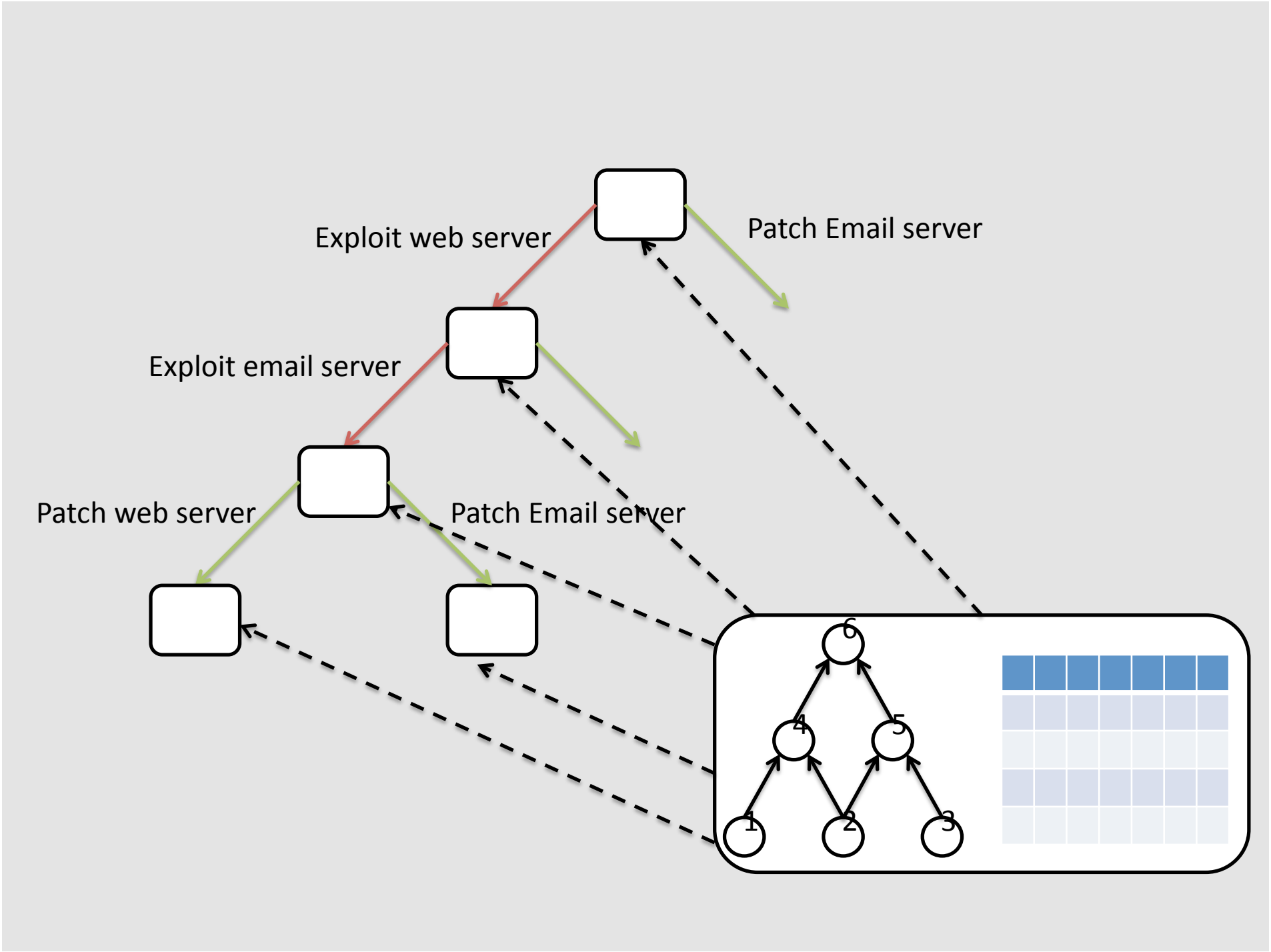
The upper layer called anticipation game is used to model the network evolution

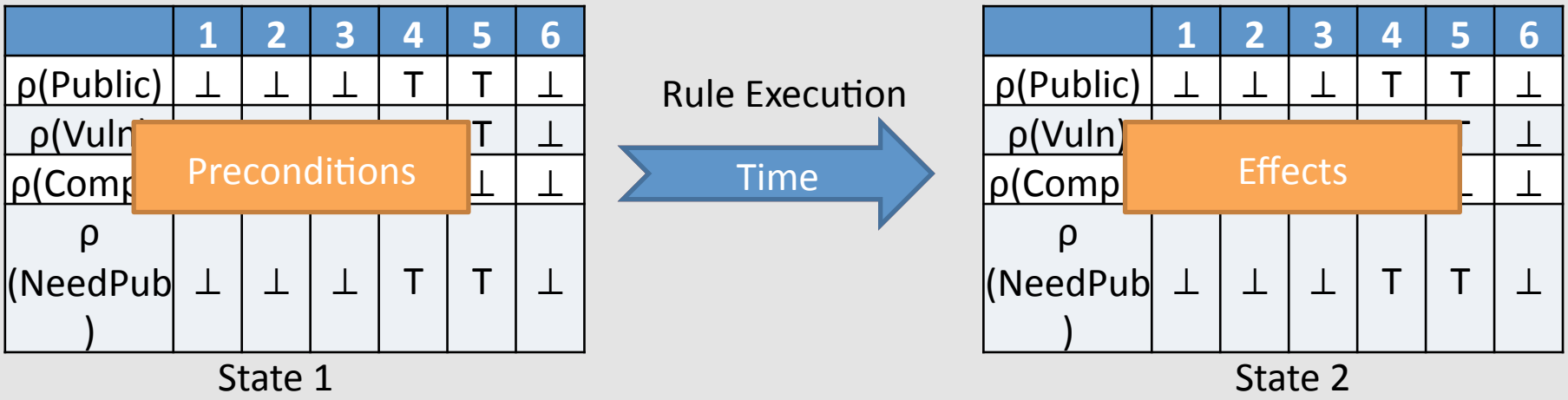


	1	2	3	4	5	6	7
ρ(Public)	T	T	T	T	T	T	T
ρ(Vuln)	⊥	⊥	T	⊥	⊥	T	⊥
ρ(Compr)	⊥	⊥	⊥	⊥	⊥	⊥	⊥
ρ(Detected)	⊥	⊥	⊥	⊥	⊥	⊥	⊥
ρ(Monitored)	⊥	T	T	T	⊥	⊥	⊥

Loc3: Virtual

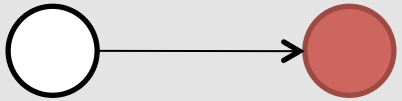
	1	2	3	4	5	6	7
ρ(Odayavail)	⊥	⊥	⊥	⊥	⊥	⊥	⊥
ρ(CustomAvail)	⊥	⊥	⊥	⊥	⊥	⊥	⊥
ρ(PubAvail)	⊥	⊥	⊥	⊥	⊥	⊥	⊥
ρ(PubPatch)	⊥	⊥	⊥	⊥	⊥	⊥	⊥

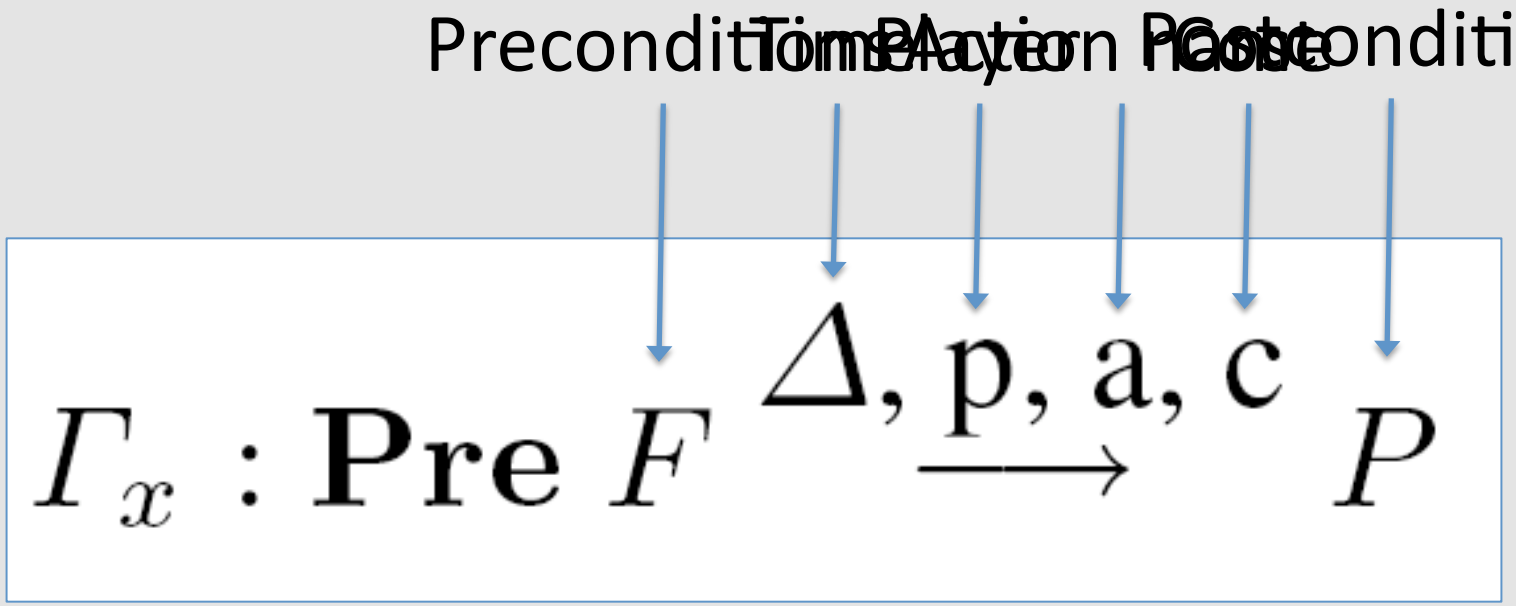

Exploit web server
Patch Email server
Exploit email server
Patch web server
Patch Email server
6
4
5
1
2
3


1 2 3 4 5 6
ρ(Public) ⊥ ⊥ ⊥ T T ⊥
ρ(Vuln) T ⊥
ρ(Comp ⊥ ⊥
ρ (NeedPub) ⊥ ⊥ ⊥ T T ⊥
Preconditions
State 1
Rule Execution
Time
1 2 3 4 5 6
ρ(Public) ⊥ ⊥ ⊥ T T ⊥
ρ(Vuln) ⊥
ρ(Comp ⊥ ⊥
ρ (NeedPub) ⊥ ⊥ ⊥ T T ⊥
Effects
State 2

$$
\begin{array}{lll}
F ::= A & & \text{atomic propositions, in } \mathcal{A} \\
\quad | \quad \top & & \text{true} \\
\quad | \quad \neg F & & \text{negation} \\
\quad | \quad F \wedge F & & \text{conjunction} \\
\quad | \quad \Diamond F & &
\end{array}
$$

$\vdash \Diamond Compr$ A successor node is compromised

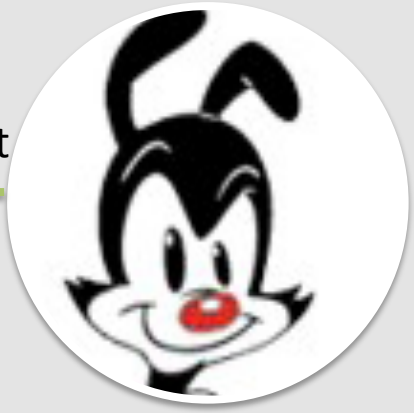



Preconditions
Time
Action
Post conditions
$\Gamma_x : \mathbf{Pre}\ F \xrightarrow{\Delta, \mathrm{p}, \mathrm{a}, \mathrm{c}} P$

Exploit 4 in 3 unit

Network

Firewall 4 in 1 unit



I. Background
II. Framework
III. Location
IV. Timeline
V. Penalty

Location

The highest form of generalship is to balk the enemy's plans

Sun Tzu, The art of war VIII.31

Rules by definition can be applied to any vertex

Sometime you need to be able to restrict their scope

Scope restriction are enforced by

location

A rule is global if no location is specified

1) $\Gamma_:$: **Pre** : $\Diamond 0DayAvail \wedge Vuln \wedge Public \wedge \neg Compr$
$\Longrightarrow$ 3, I, 0 day exploit, 20000
Effect : $Compr$

2) $\Gamma_:$: **Pre** : $\Diamond CustomAvail \wedge Vuln \wedge Public \wedge \neg Compr$
$\Longrightarrow$ 4, I, Custom exploit, 2000
Effect : $Compr$

3) $\Gamma_:$: **Pre** : $\Diamond PubAvail \wedge Vuln \wedge Public \wedge \neg Compr$
$\Longrightarrow$ 7, I, Public exploit, 200
Effect : $Compr$

A rule is local if the same location is specified for the node and its successors

4) $\Gamma_{3:3}$: **Pre** : $\neg Compr \wedge \Diamond Compr$
$\Longrightarrow$ 2, I, Trust Abuse, 200
Effect : $Compr$

5) $\Gamma_{1:1}$: **Pre** $Monitored \wedge Compr \wedge \neg Detected$
$\longrightarrow$ 1, A, Attack Detected, 2000
Effect $Detected$

6) $\Gamma_{2:2}$: **Pre** $\neg Vuln \wedge \neg Public$
$\longrightarrow$ 1, A, Unfirewall, 100
Effect $Public$

A rule is transitive if a different location is specified for the node and its successors

7) $\Gamma_{3:2}$: **Pre** $\Diamond Detected \wedge Vuln \wedge Public$
$\longrightarrow$ 0, A, Firewall, 100
Effect $\neg Public$

8) $\Gamma_{3:1}$: **Pre** $\Diamond PatchAvail \wedge Vuln$
$\longrightarrow$ 6, A, Patch, 500
Effect $\neg Vuln$

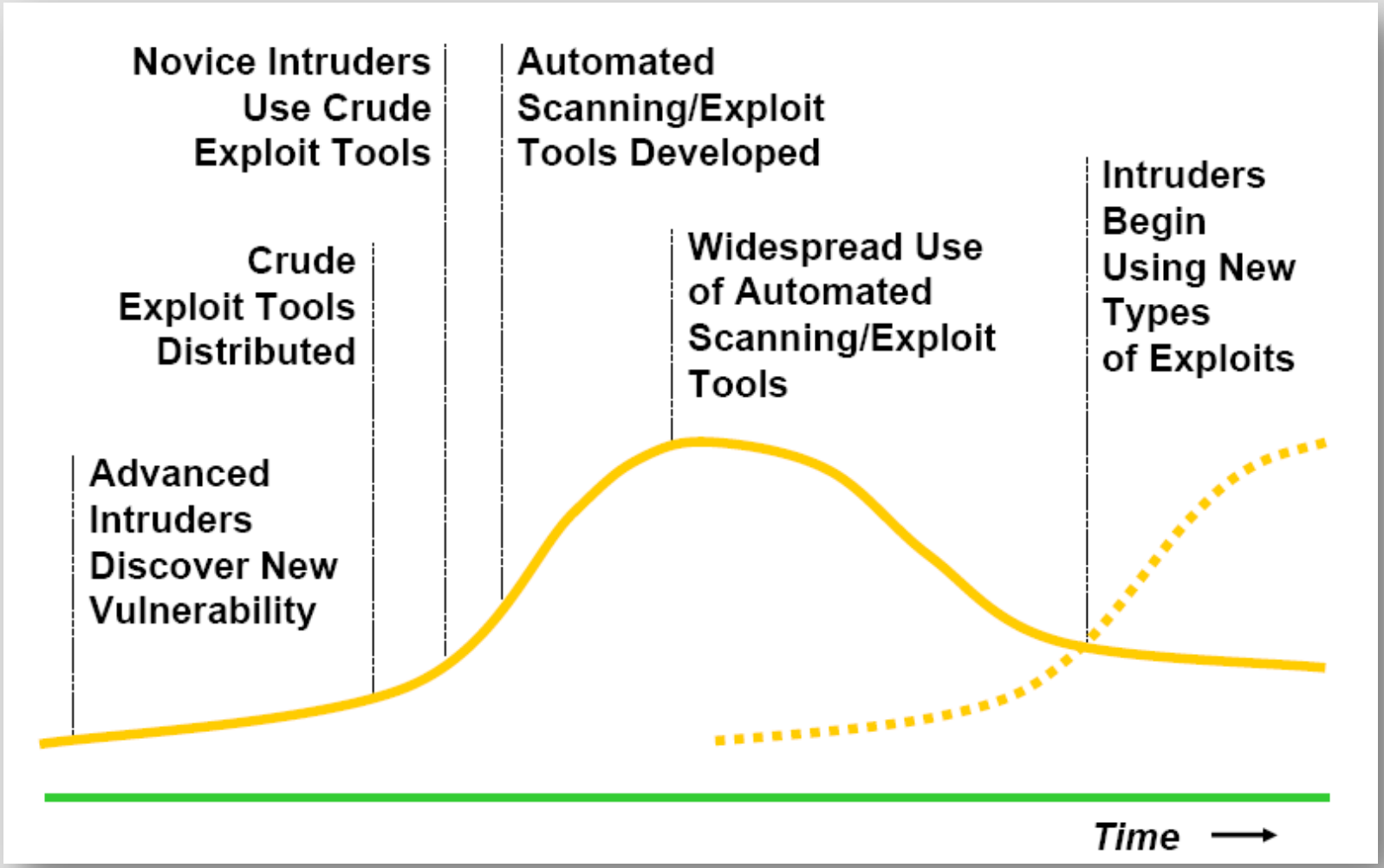
I. Background
II. Framework
III. Implementation
IV. Applications

Timeline

Success in warfare is gained by carefully accommodating ourselves to the enemy's purpose.

Sun Tzu, The art of war IV.13

In order to express a causal relation between action we need to be able to model a timeline


Novice Intruders Use Crude Exploit Tools
Automated Scanning/Exploit Tools Developed
Intruders Begin Using New Types of Exploits
Widespread Use of Automated Scanning/Exploit Tools
Crude Exploit Tools Distributed
Advanced Intruders Discover New Vulnerability
Time

1) $\Gamma_{1:1}$: **Pre** $\neg 0DayAvail$
$\longrightarrow$ 48, I, O day exploit Available, 0
Effect $0dayAvail$

2) $\Gamma_{1:1}$: **Pre** $\neg CustomAvail \wedge 0DayAvail$
$\longrightarrow$ 288, I, Custom exploit available, 0
Effect $CustomAvail$

3) $\Gamma_{1:1}$: **Pre** $\neg PubAvail \wedge CustomAvail$
$\longrightarrow$ 48, I, Public exploit available, 0
Effect Pub

4) $\Gamma_{1:1}$: **Pre** $\neg PatchAvail \wedge CustomAvail$
$\longrightarrow$ 48, I, Patch available, 0
Effect $0dayAvail$

I. Background
II. Framework
III. Implementation
IV. Applications

Penality

To secure ourselves against defeat lies in our own hands

Sun Tzu, The art of war IV.2

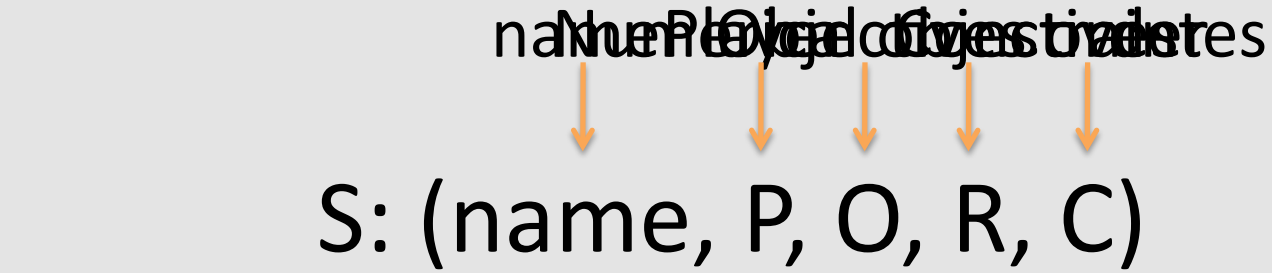
A Penalty allows to add a duration based cost

Model-checking anticipation game with location and penalty is EXPTIME-Complete

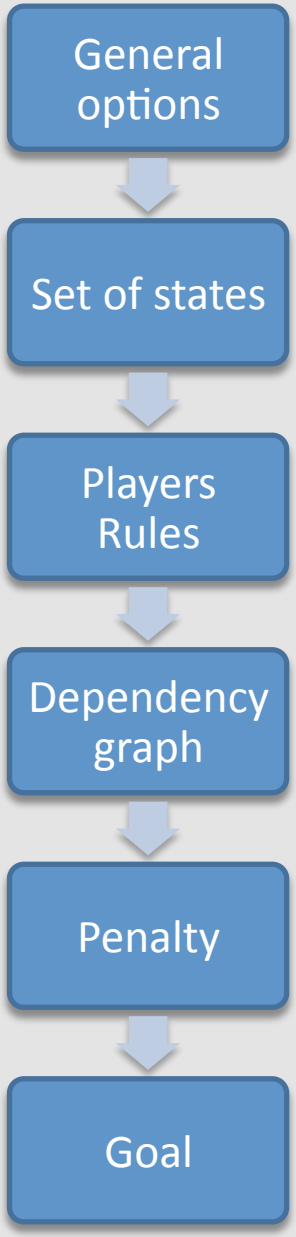
A counter-example is an attack and there can be a lot of counter-example

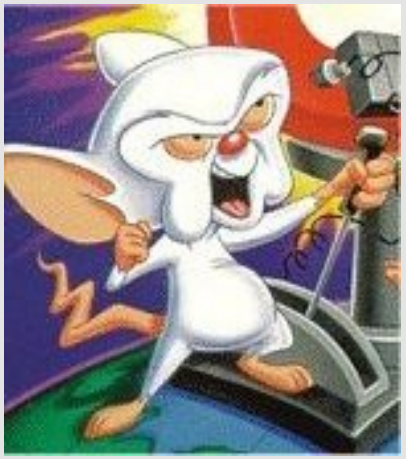
How do you know which counter-example is the most relevant one?

Strategy objectives mix constraints with costs and rewards


name
S: (name, P, O, R, C)

$$S : (\text{Defense strategy}, Admin, MIN(Cost) \wedge MAX(OCost), OCost > Cost, \Box\neg Compr, \neg 2)$$


General options
Set of states
Players Rules
Dependency graph
Penalty
Goal



Demonstration

Analysis	services	Network	Time
Exact	30	3	0.03
Exact	40	3	0.1
Exact	20	4	1020
Approx	2000	1	0.48
Approx	5000	4	0.82
Approx	10000	3	2.26

Conclusion

If you know the enemy and know yourself, your victory will not stand in doubt; if you know Heaven and know Earth, you may make your victory complete.

Sun Tzu, The art of war VIII.31

$$\varphi ::= A \qquad \text{Atomic proposition}$$
$$\mid \quad \neg\varphi$$
$$\mid \quad \varphi \wedge \varphi$$
$$\mid \quad \forall A$$
$$\mid \quad \exists A$$
$$\mid \quad \Box\varphi$$
$$\mid \quad \Diamond$$

Ts	Pl	Ac	Rule	Ta	S	Pa	C
0	I	sel	0day avail	2	$\perp$	-	-
48	I	**exec**	0day avail	2	$\perp$	0	0
48	I	sel	Custom avail	2	$\perp$	-	-
336	I	**exec**	Custom avail	2	$\perp$	0	0
337	I	sel	Public avail	2	$\perp$	-	-
337	A	sel	Patch avail	2	$\perp$	-	-
385	I	**exec**	Public avail	2	$\perp$	0	0
385	I	sel	Compr public	7	2	-	-
385	A	**exec**	Patch avail	2	$\perp$	0	2700
385	A	sel	Patch	7	2	-	-
391	A	**exec**	Patch	7	2	1	3500
392	I	`fail`	Compr public	7	2	0	200

Ts	Pl	Ac	Rule	Ta	S	Pa	C
0	I	sel	0day avail	2	$\perp$	-	-
48	I	**exec**	0day avail	2	$\perp$	0	0
48	I	sel	Compr 0 day	4	2	-	-
51	I	**exec**	Compr 0 day	4	2	1	20000
52	I	sel	Compr 0 day	7	2	-	-
52	A	sel	Attack catched	4	$\perp$	-	-
52	A	**exec**	Attack catched	4	$\perp$	0	2000
52	A	sel	Firewall	7	4	-	-
52	A	**exec**	Firewall	7	4	0	4800
54	I	`fail`	Compr 0 day	7	2	1	40000
54	I	sel	Custom avail	2	$\perp$	-	-
342	I	**exec**	Custom avail	2	$\perp$	1	40000
343	I	sel	Public avail	2	$\perp$	-	-
343	A	sel	Patch avail	2	$\perp$	-	-
390	I	**exec**	Public avail	2	$\perp$	1	40000
391	A	**exec**	Patch avail	2	$\perp$	0	4000
391	A	sel	Patch	7	2	-	-
397	A	**exec**	Patch	7	2	1	4500
397	A	sel	UnFirewall	7	$\perp$	-	-
398	A	**exec**	UnFirewall	7	$\perp$	1	4803