NetQi

Elie Bursztein
LSV, ENS-Cachan

I. Background
II. Model
III. Tool

NetQi name come from the English word *Net* and the Chinese word Qi : 氣 which mean vital energy flow

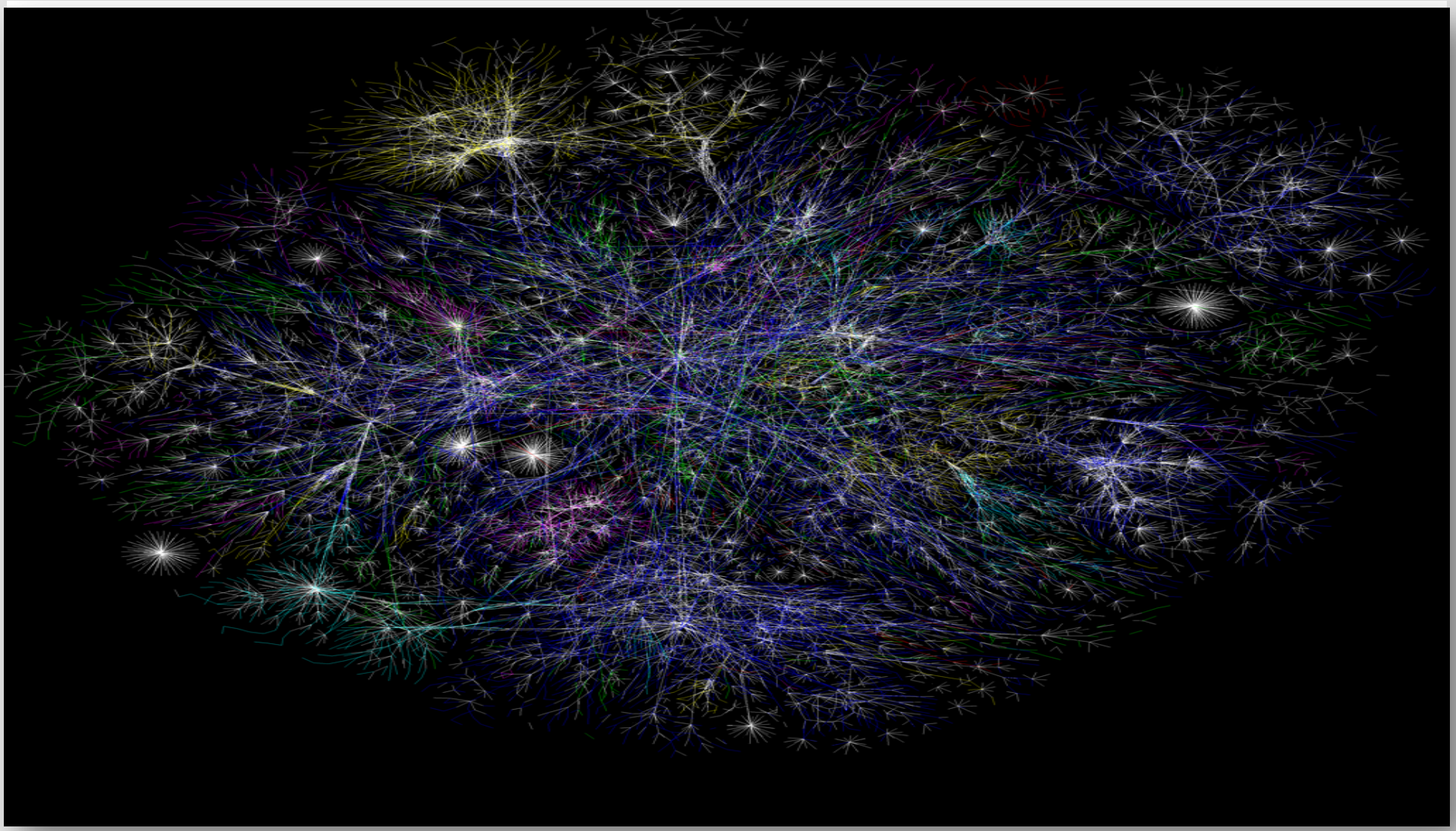
I. Background
II. Model
III. Tool

Background

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

Sun Tzu, The art of war I.1

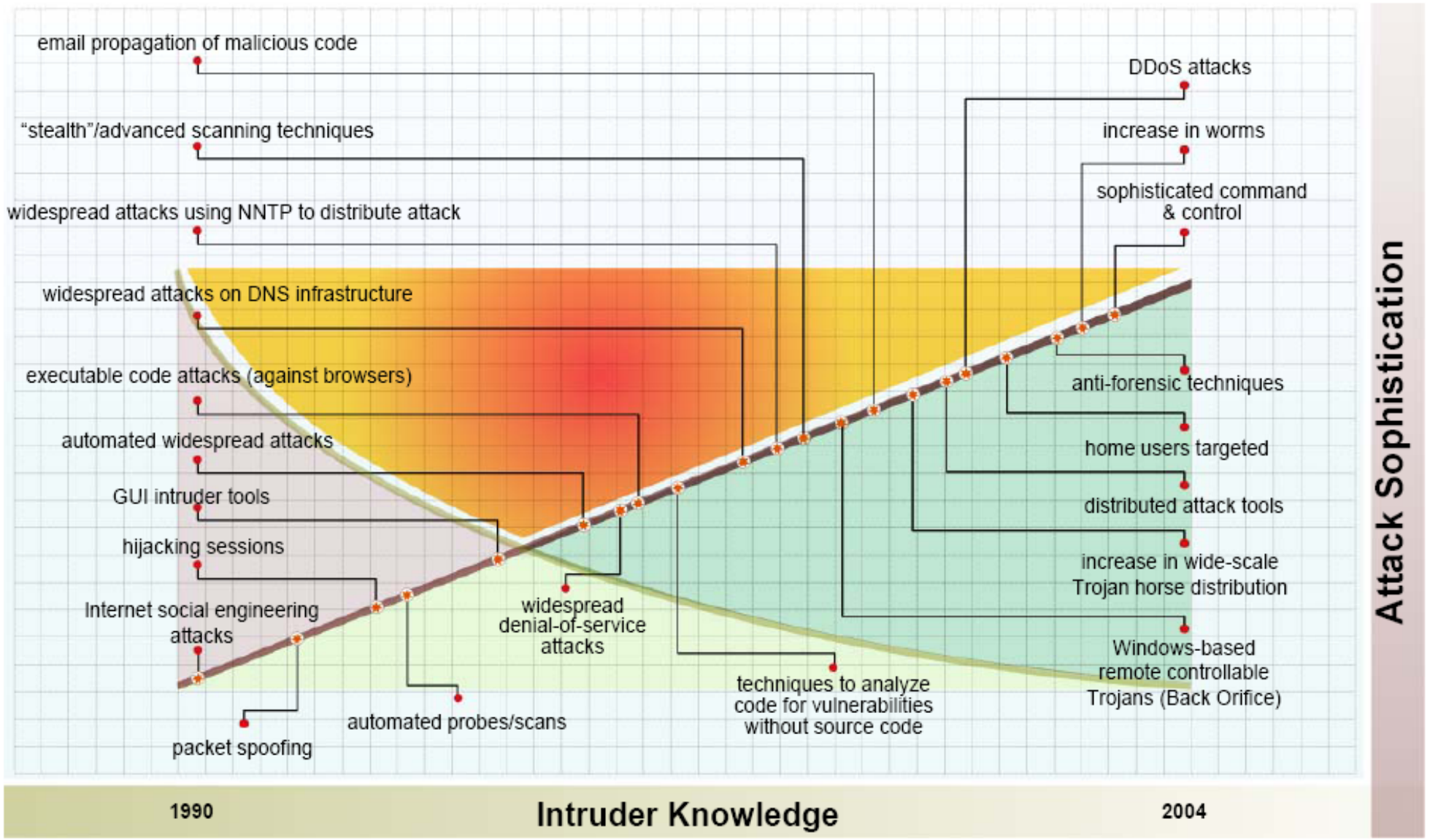
Network is getting more and more complex



Opte project

1 400 000 000 people use internet

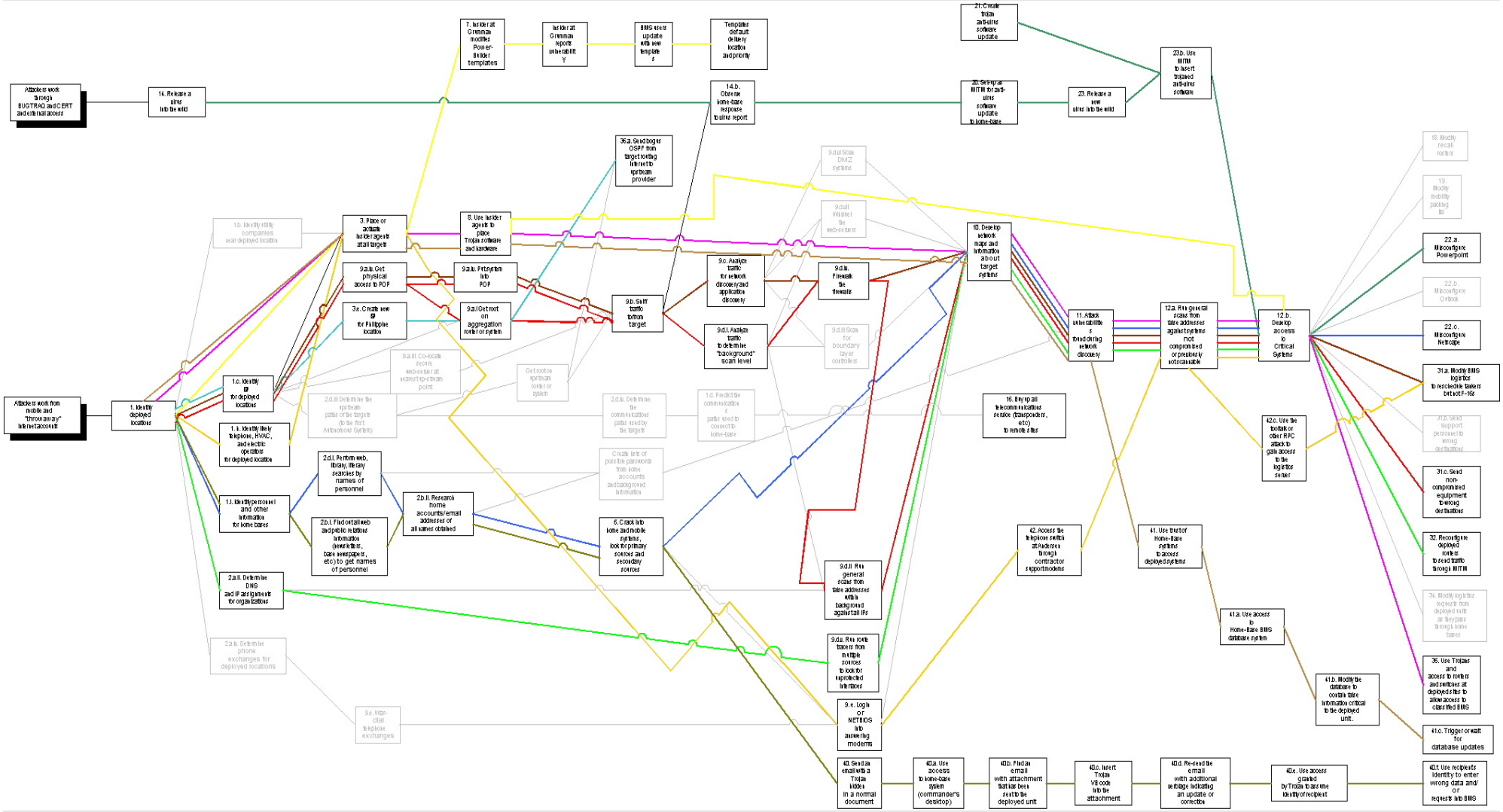
Attack techniques are getting more and more sophisticated



Cert/ Carnegie Mellon University

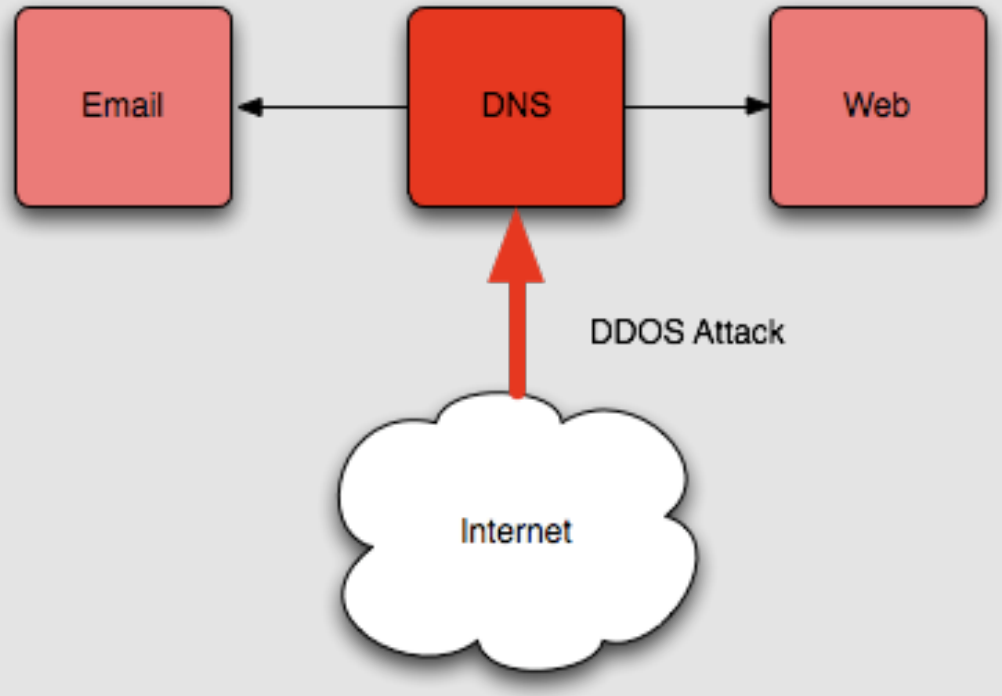
40 000 vulnerabilities will be in the wild before the end of 2008

The survival time of a window XP connected to Internet is 5 minutes



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

Take into account the collateral damages



Exploit vulnerabilities

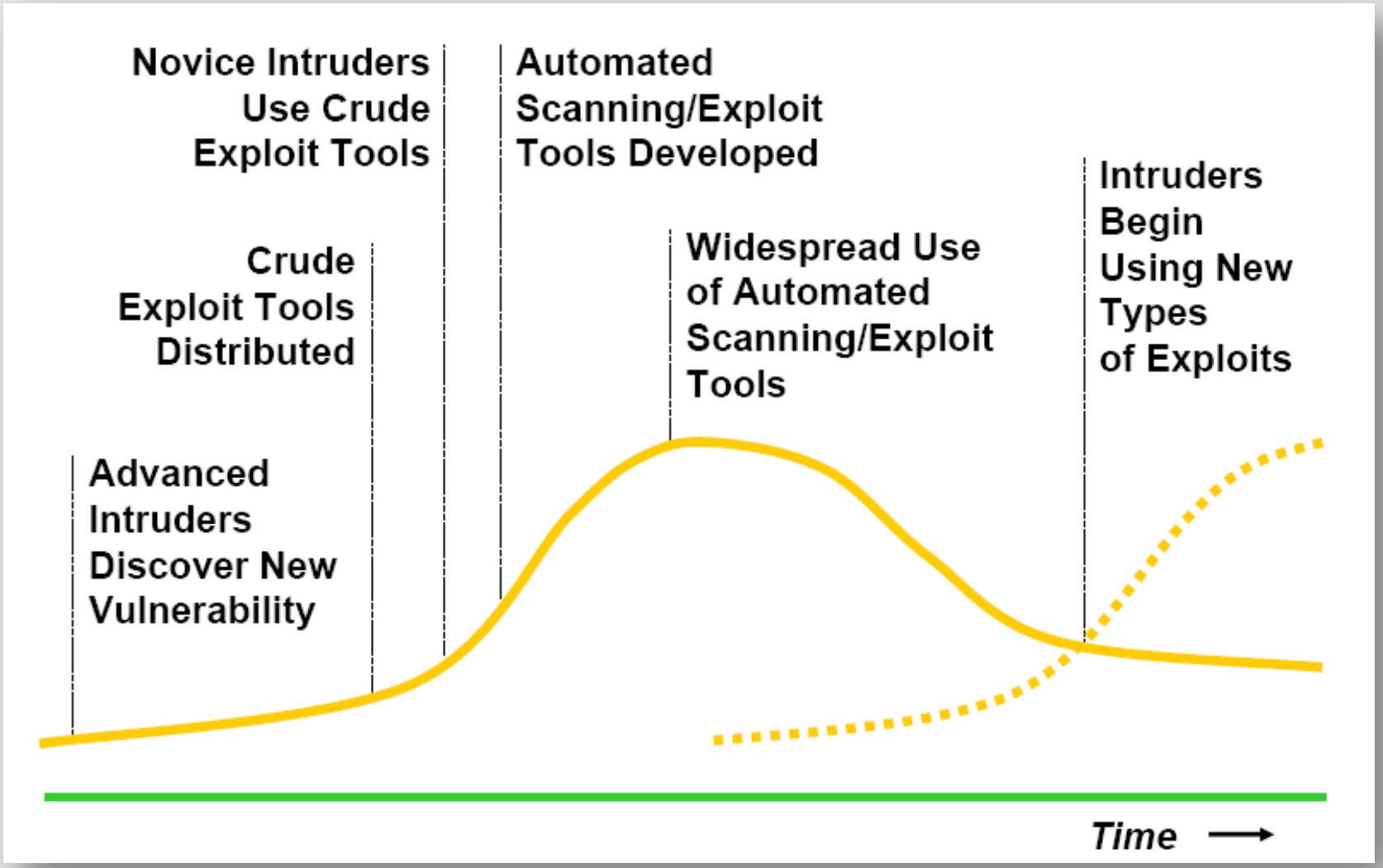
Abuse trust relations

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 that well

Constructing the model is a challenge

I. Background
II. Model
III. Tool

Model

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

Sun Tzu, The art of war II.19

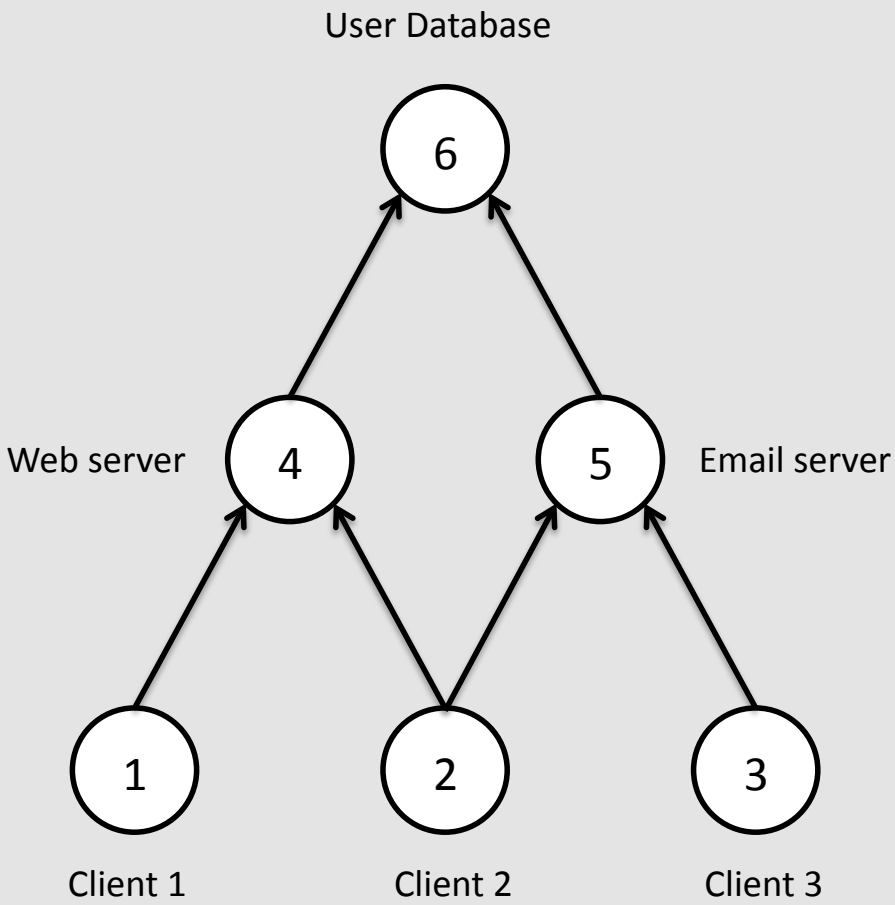
Its is based on game theory TATL and modal logic

its model is called Anticipation Game

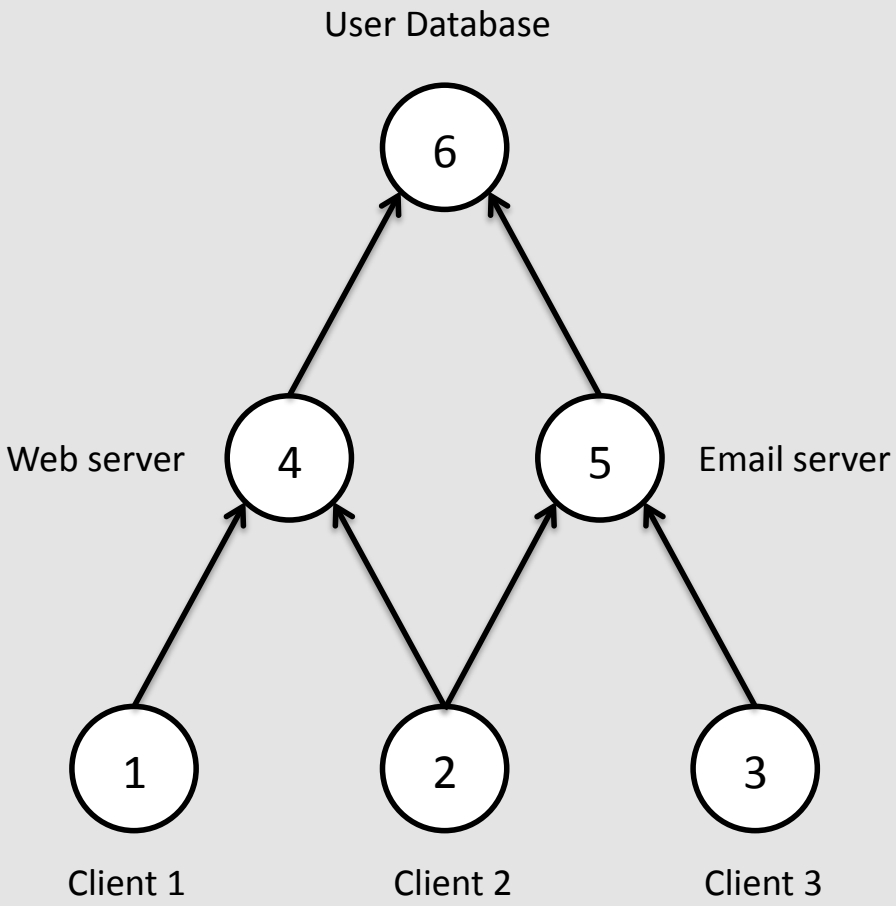
An anticipation game is a dual layer structure

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

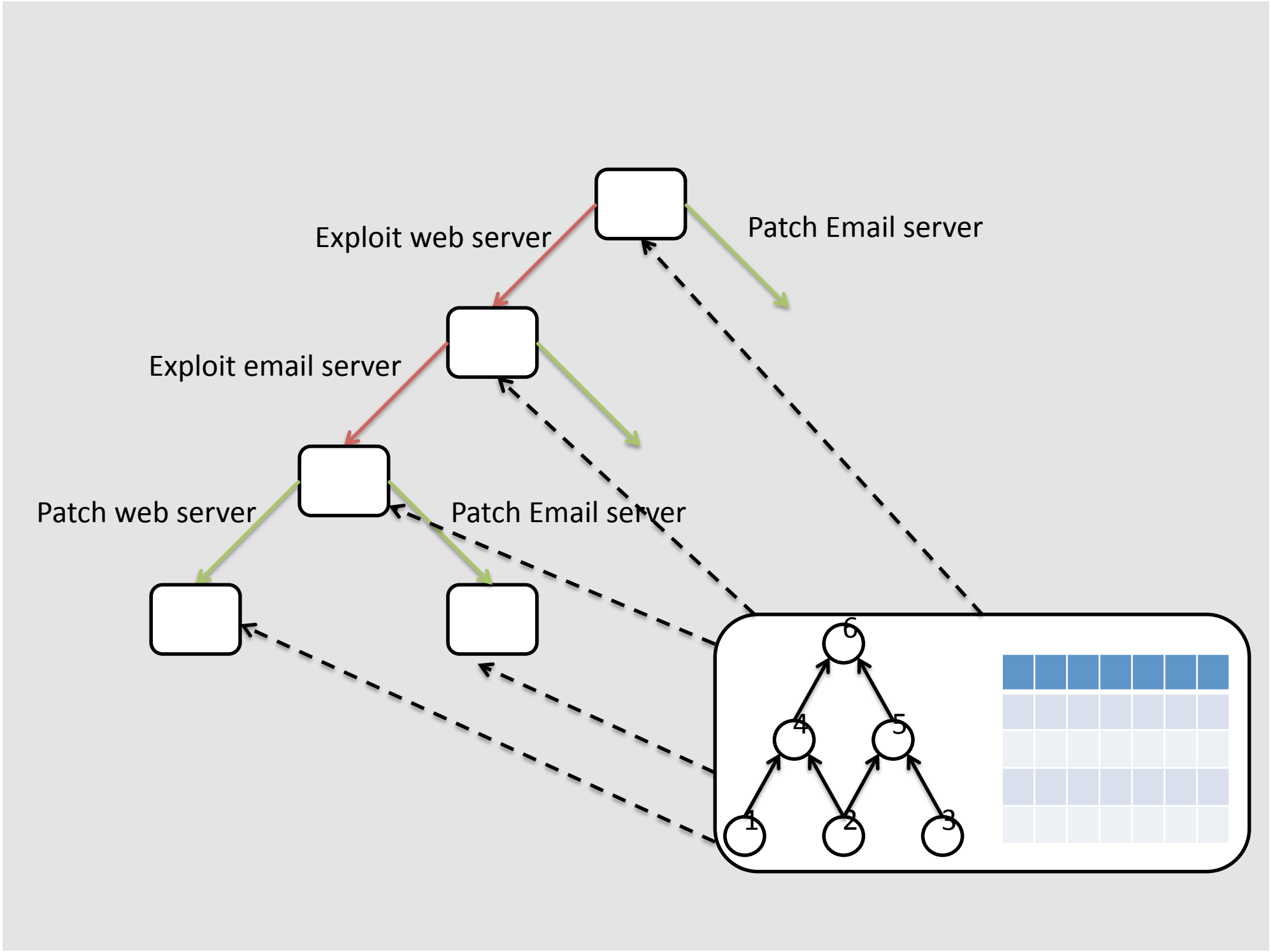

User Database
6
Web server
4
5
Email server
1
2
3
Client 1
Client 2
Client 3

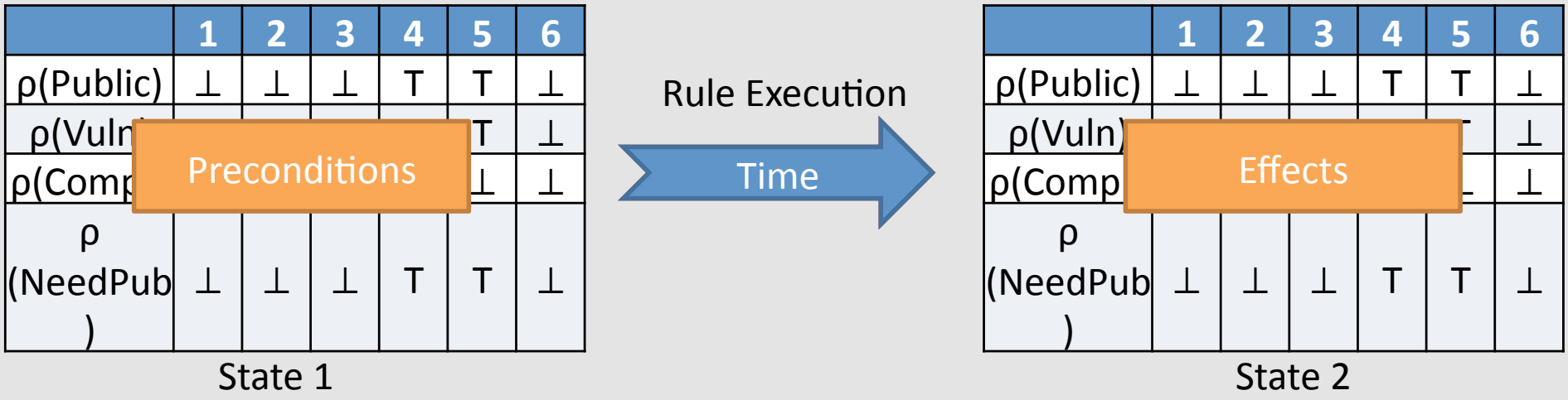
Fixed over the time

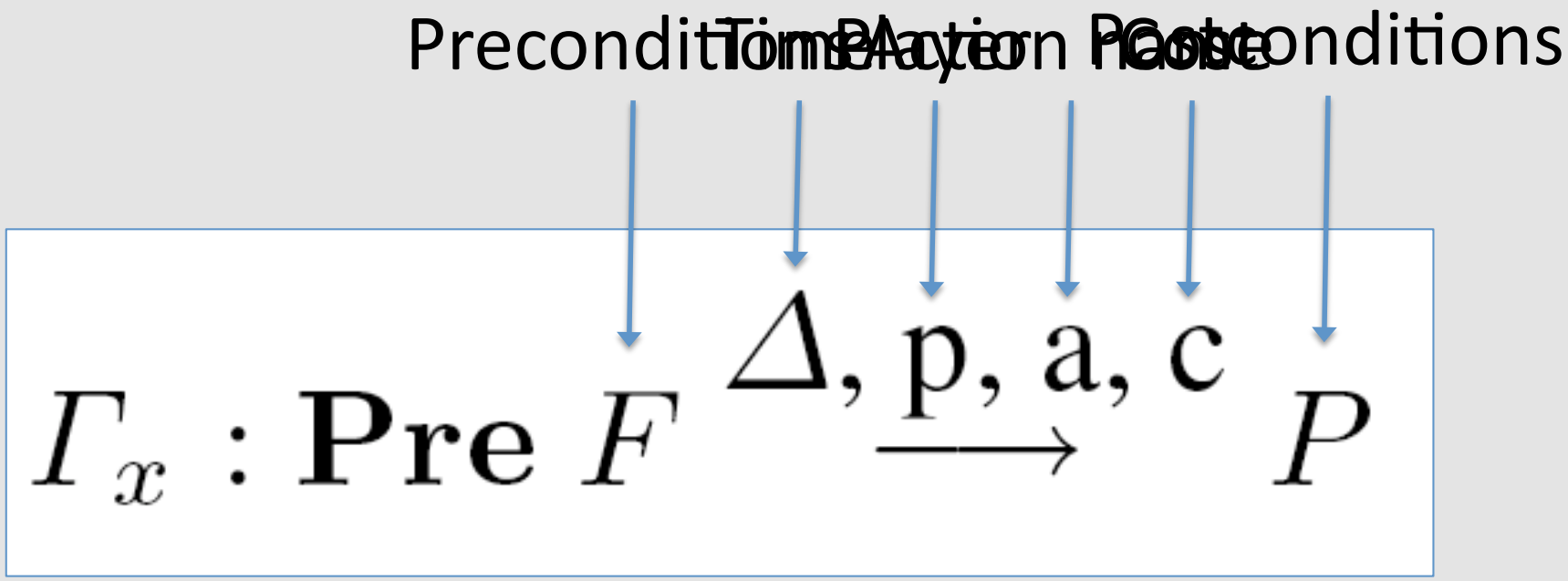


Evolve over time

	1	2	3	4	5	6
ρ(Public)	⊥	⊥	⊥	T	T	⊥
ρ(Vuln)	⊥	⊥	⊥	T	T	⊥
ρ(Compr)	⊥	⊥	⊥	⊥	⊥	⊥
ρ(NeedPub)	⊥	⊥	⊥	T	T	⊥

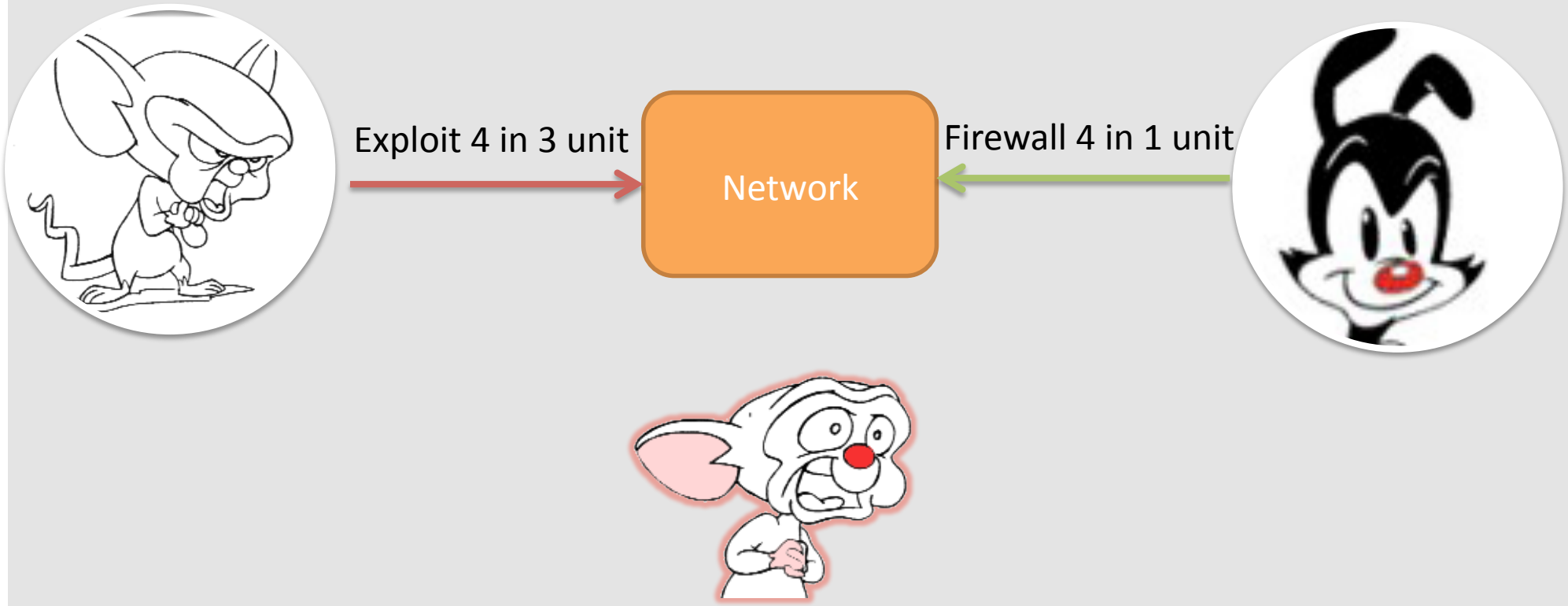

Exploit web server
Patch Email server
Exploit email server
Patch web server
Patch Email server
6
4
5
1
2
3


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


Precondition
Time
Action
Parameters
Probability
Cost
Postconditions
$\Gamma_x : \mathbf{Pre}\ F \xrightarrow{\Delta, \mathrm{p}, \mathrm{a}, \mathrm{c}} P$

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

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


Exploit 4 in 3 unit
Network
Firewall 4 in 1 unit

Model-checking TATL formula on anticipation 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

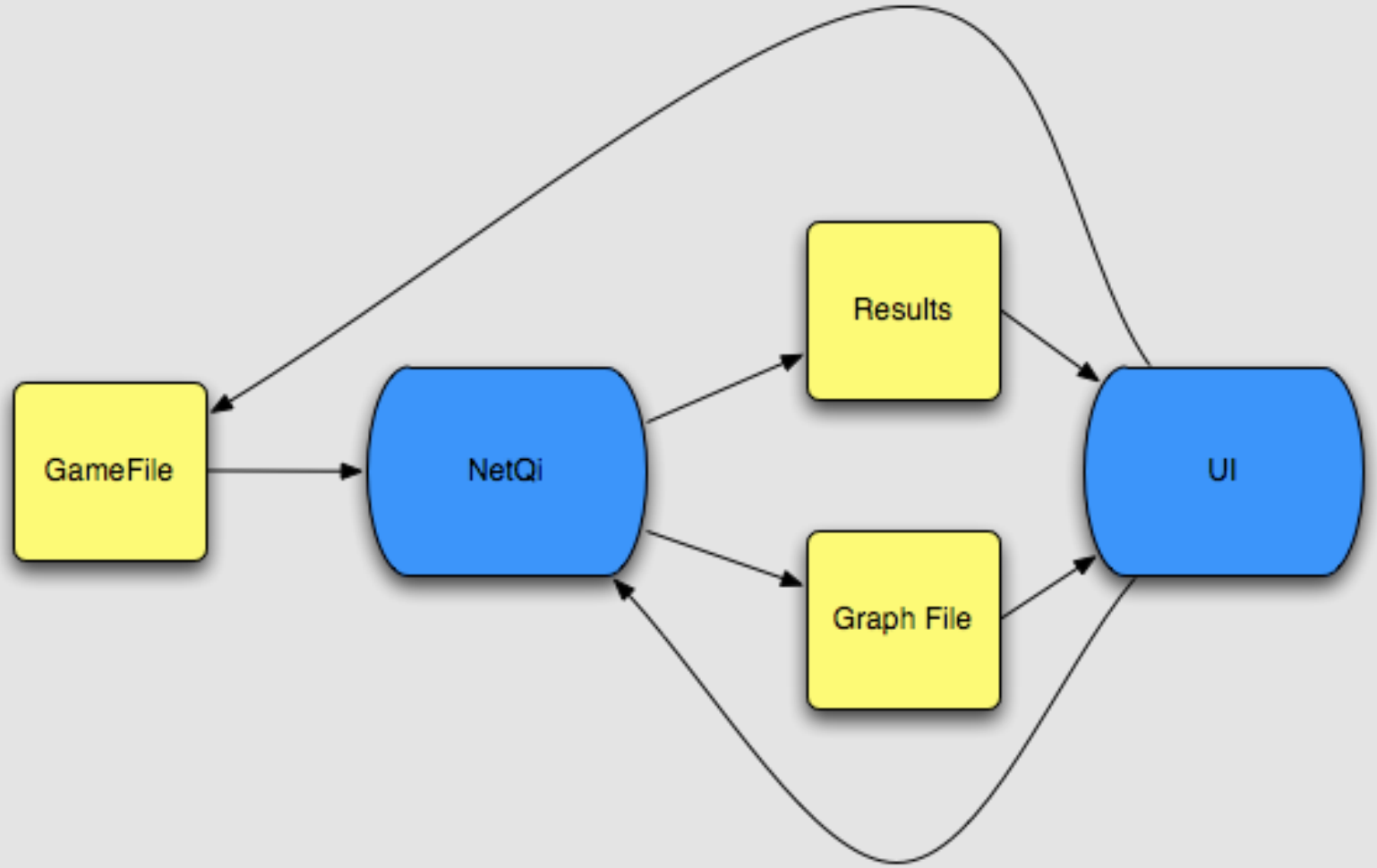
I. Background
II. Model
III. Tool

Tool

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

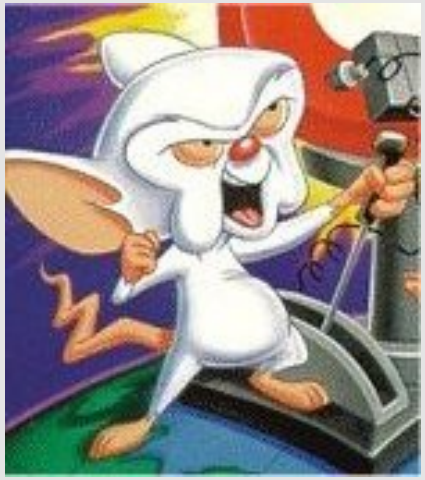
Sun Tzu, The art of war VIII.31

NetQi




网氣 NetQi
Brings foresight to your world
Home
News
Download
Documentation
About
Screenshots
Contact us
What Is Netqi ?
NetQi name come from the English word Net and the Chinese word Qi : 氣 which mean vital energy flow. Hence NetQi is a tool designed to analyze the "network vital energy flow" to prevent attacks and failures that can harm this flow (legitimate traffic). It is based on timed game and model-checking theory.
So far it has been successfully used to analyze many network security threats including: Distributed Denial Of Service (DDOS), Network Exploit, Trust Relation Abuse, Information Leak, Password Cracking, Hard drive crash and DNS cache poisoning.
NetQi is not limited to network security and can be used to analyze most situation where interaction with a complex environment can be described as rules such as protein interaction in biology.
Learn how NetQi can help you
Download
The NetQi tools are Open-Source and free for non-commercial applications in academia, research, and for private persons. For commercial applications a commercial license is required.
Download
Type and Wait to Search
Recent News
NetQi presented at MITACS
Version 1.1
Version 1.0
Paper Published at ASIAN 2007: A Logical Framework for Evaluating Network Resilience Against Faults and Attacks
Affiliations
Laboratoire Spécification et Vérification
ENS CACHAN
CNRS
INRIA FUTURS

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



Demonstration

网氣 NetQi

Brings foresight to your world

www.netqi.org

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

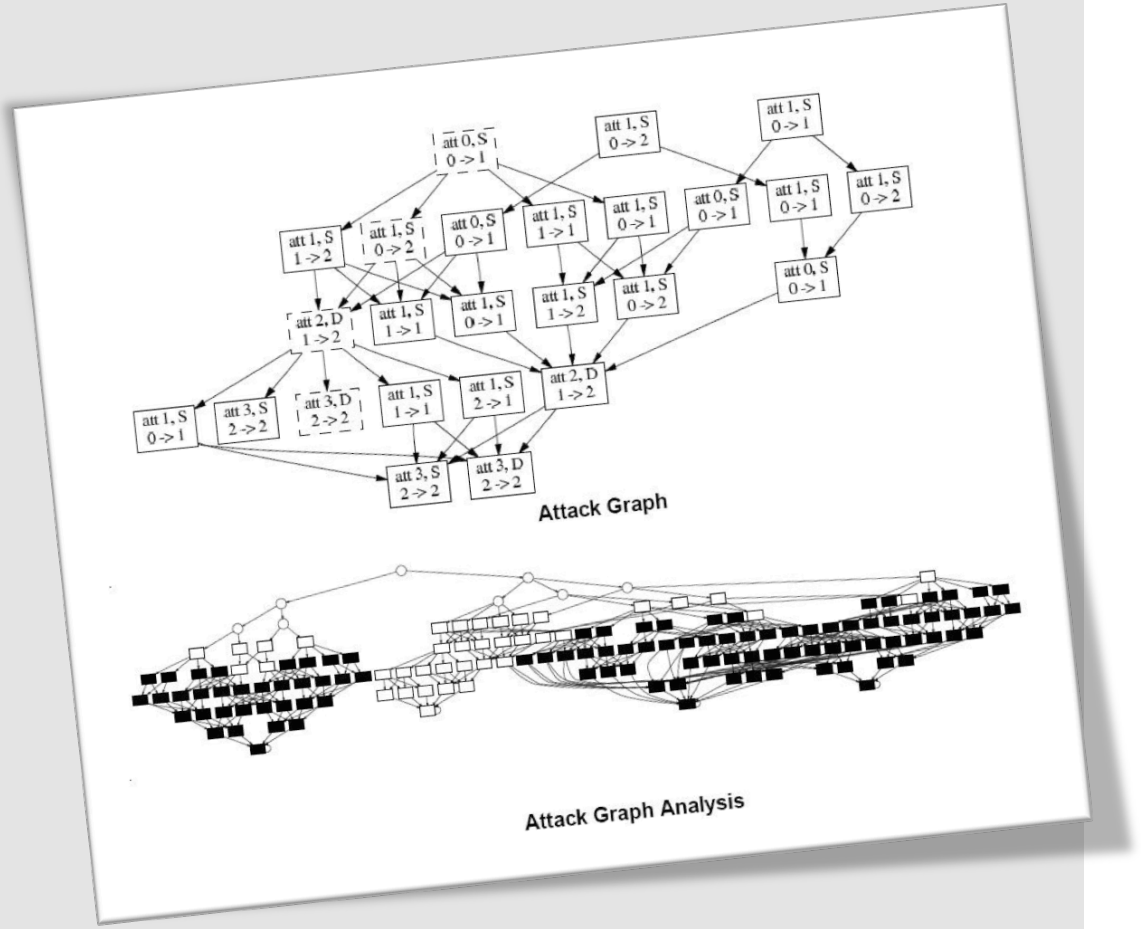
$$S : (\text{Defense strategy}, Admin, MIN(Cost) \wedge MAX(OCost), OCost > Cost, \Box\neg Compr, \neg 2)$$

its a 4th generation* framework

*Baskerville classification 1993

Previous framework

- Attack graph
- NetSpa
- MulVal
- Cauldron



SEIR model

$$
\begin{aligned}
\varphi ::= {} & A && \text{Atomic proposition} \\
\mid {} & \neg\varphi \\
\mid {} & \varphi \wedge \varphi \\
\mid {} & \forall A \\
\mid {} & \exists A \\
\mid {} & \Box\varphi \\
\mid {} & \Diamond
\end{aligned}
$$

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