Elie Bursztein
eb@lsv.ens-cachan.fr

Anticipation Games

Elie Bursztein
Phd Student LSV ENS-CACHAN CNRS INRIA DGA

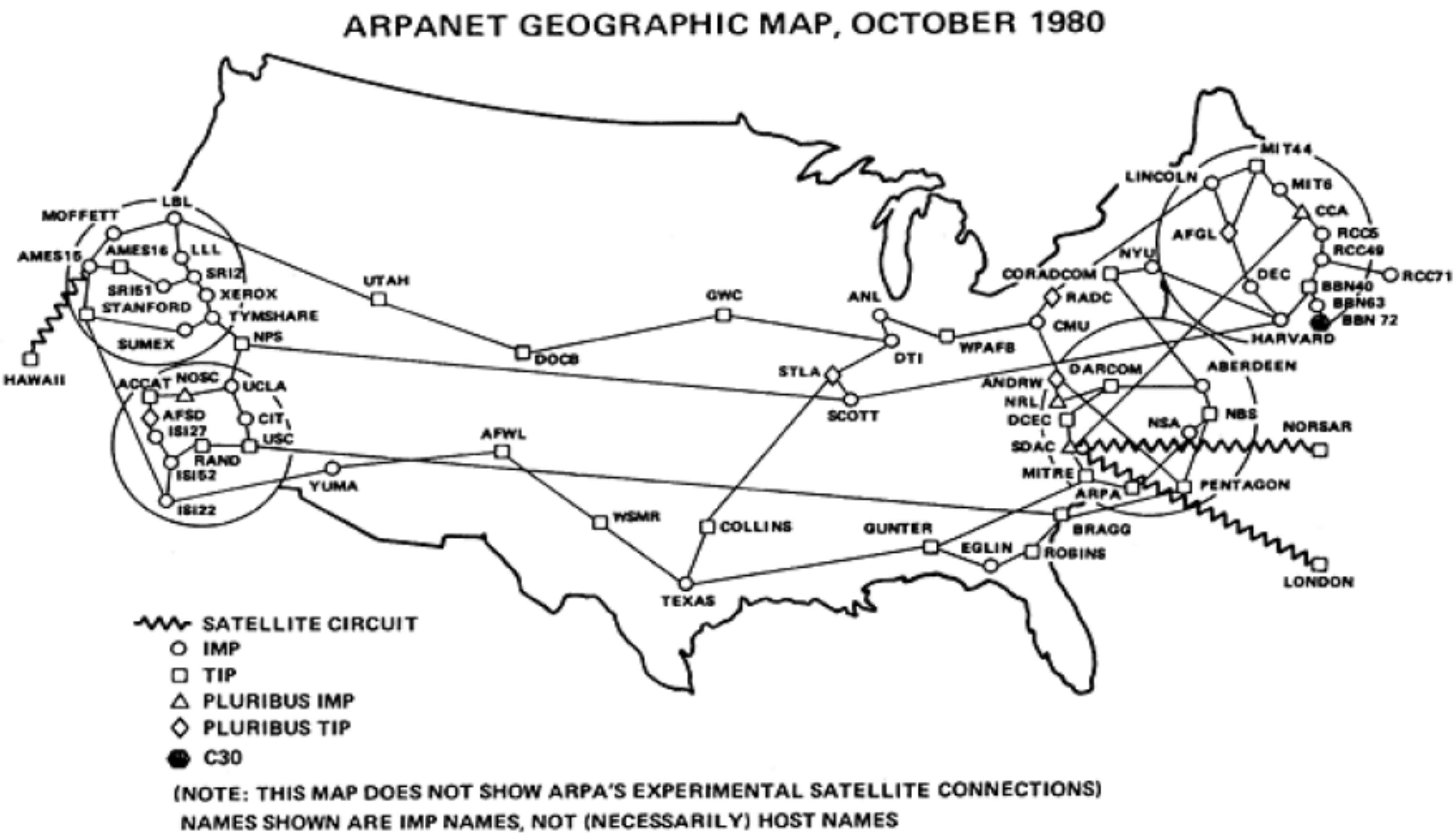
Outline

Elie Bursztein
eb@lsv.ens-cachan.fr

- Introduction
  - Network Evolution
  - Attack Model Evolution
- Anticipation game key features
  - Dependency relations
  - Player interaction
  - Time
- Model Logic
  - Positional Logic
  - Temporal Logic
- Conclusion

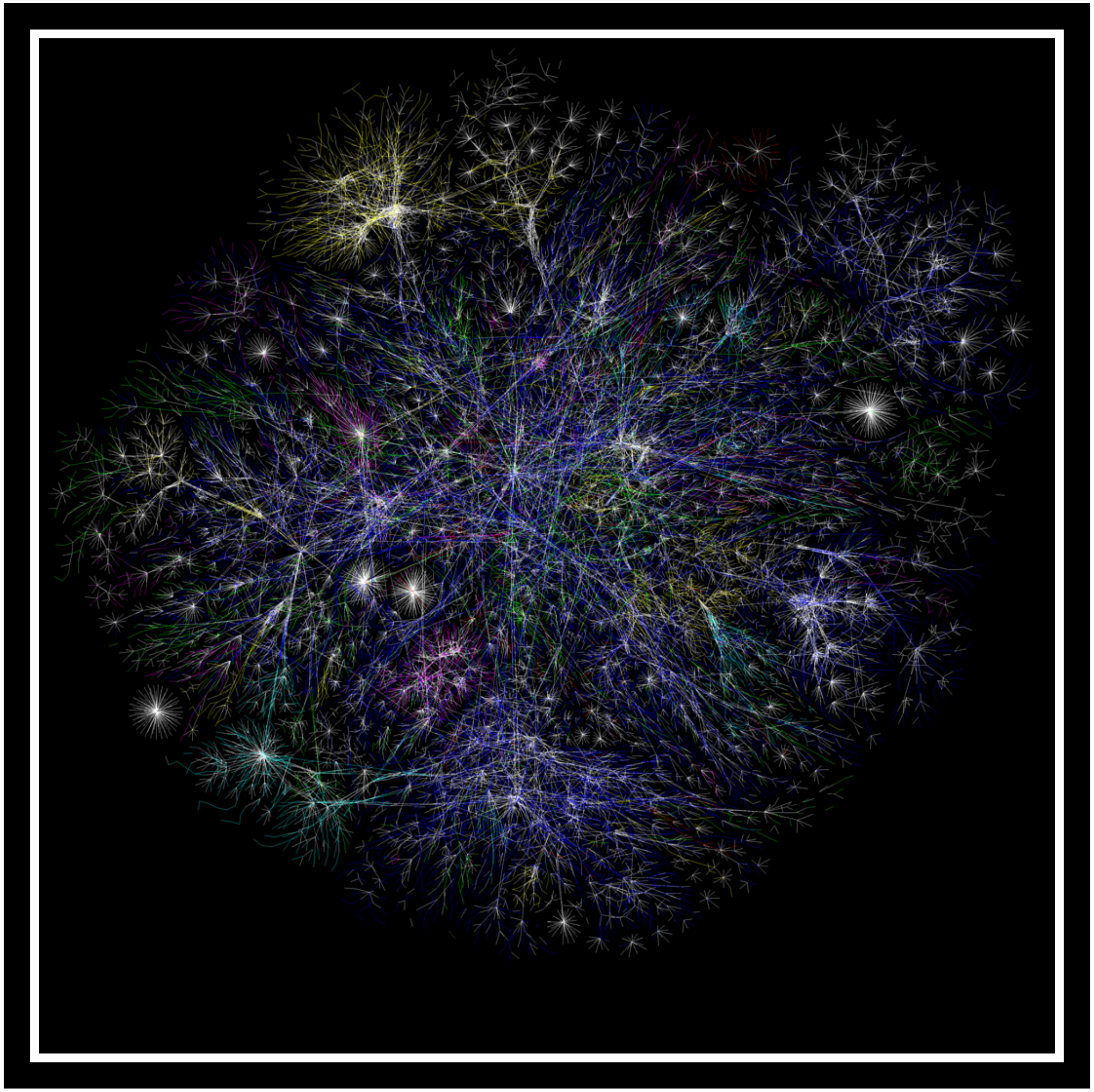
The Good Old Time

Elie Bursztein
eb@lsv.ens-cachan.fr



The Current Internet

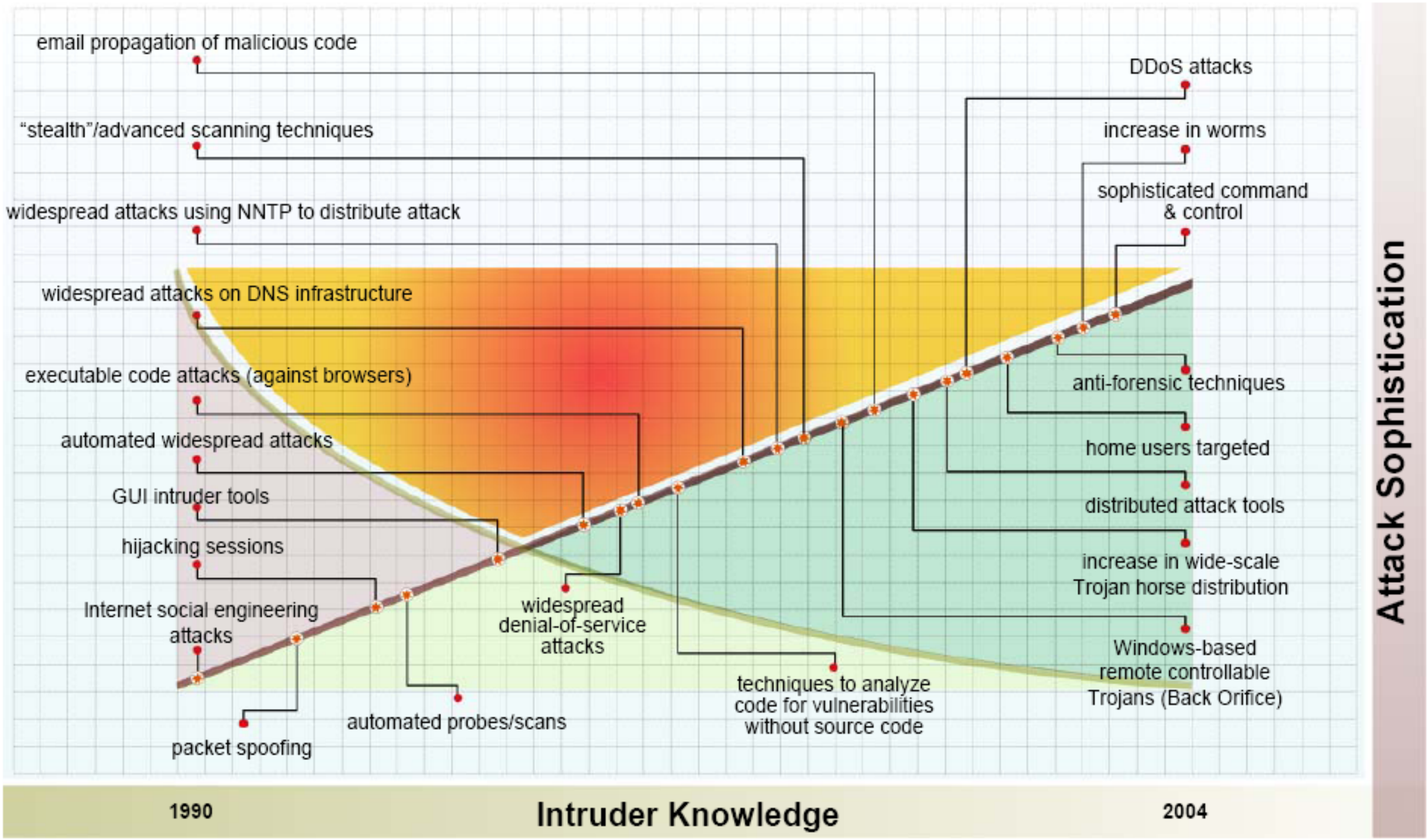
Elie Bursztein
eb@lsv.ens-cachan.fr



Opte project

Attack Sophistication vs. Intruder Knowledge

Elie Bursztein
eb@lsv.ens-cachan.fr



Cert/ Carnegie Mellon University

Attack Step-stones

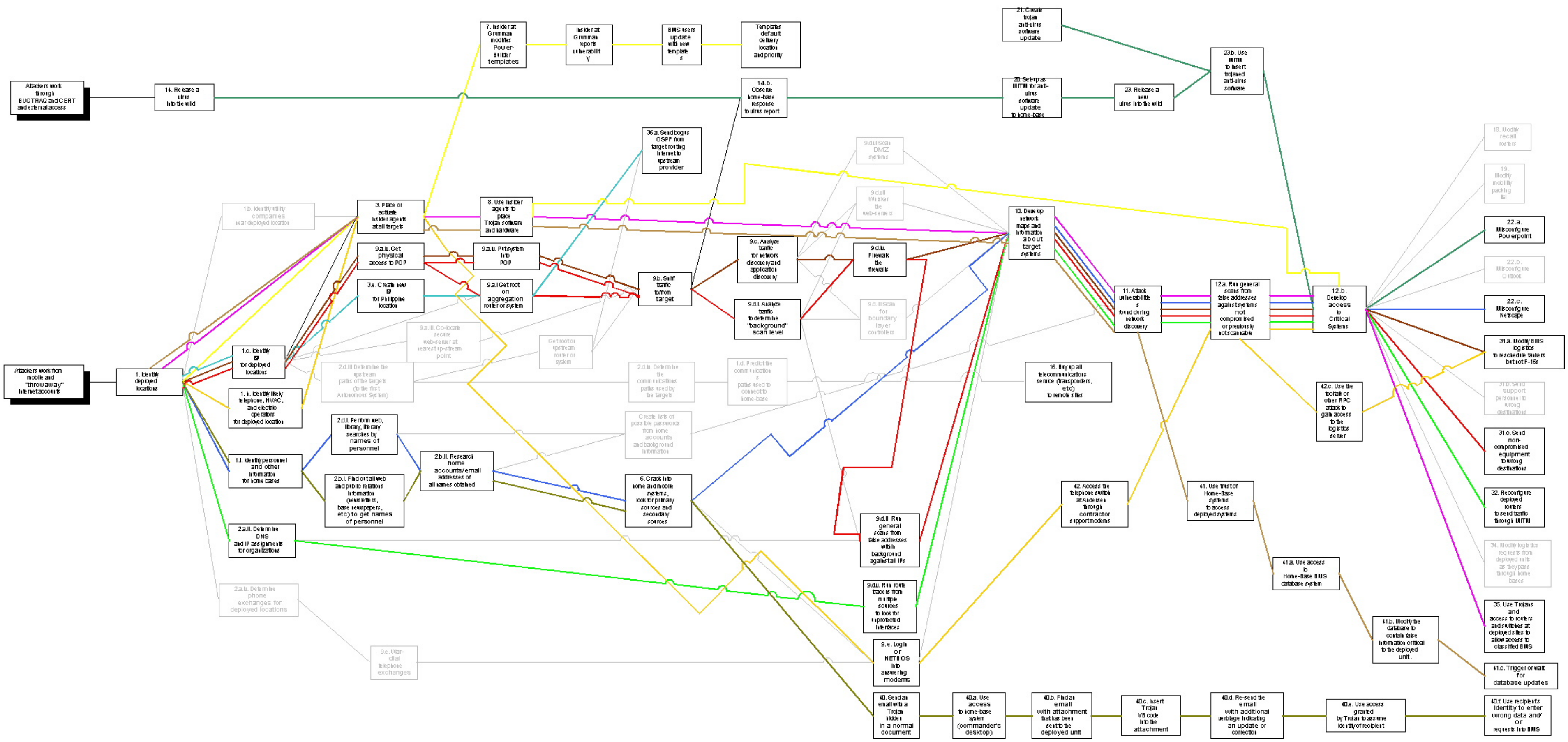
Elie Bursztein
eb@lsv.ens-cachan.fr

- Large network may suffers multiples vulnerabilities
- Patches and counter-measures need to be prioritized
- A minor vulnerability can turn into a major hole when used as a step-stone

Attack graph allows to reason about attack sequences

Attack Graph Example

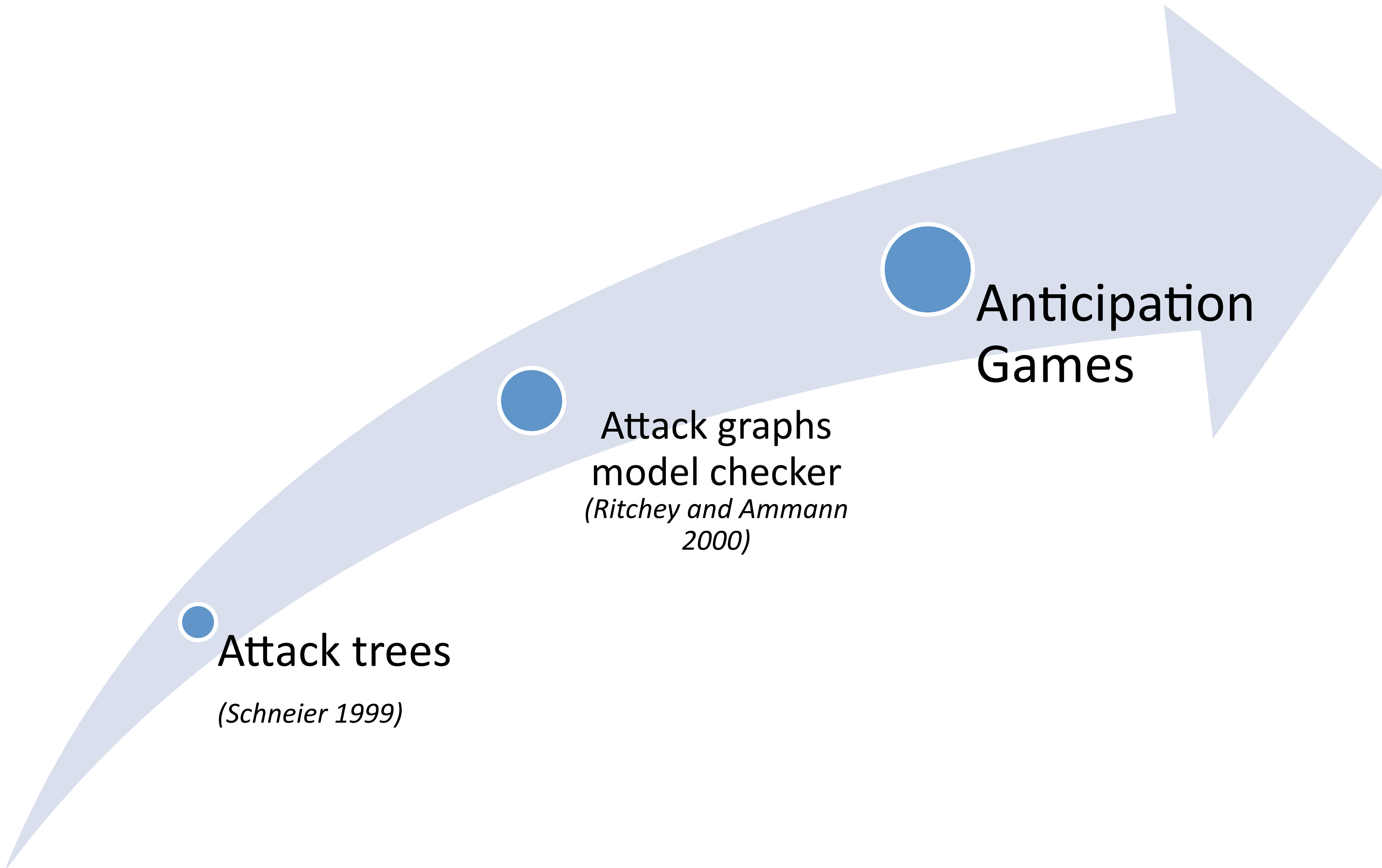
Elie Bursztein
eb@lsv.ens-cachan.fr



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

Model Evolution

Elie Bursztein
eb@lsv.ens-cachan.fr



Related Work

Elie Bursztein
eb@lsv.ens-cachan.fr

- Attack graph
  - Model checker-based (Ritchey et. al S&P'00, Sheyner et. al S&P'02)
  - Graph-based (Ammann et. al CCS'02, Ritchey et. al ACSAC'02, Noel et. al ACSAC'03, Wang et. al ESORICS'05, Wang et. al DBSEC'06)
- Timed Game
  - ATL (Alur et al. 97)
  - The Element of Surprise in Timed Games (De Alfaro et al. CONCUR 2003)
  - TATL (Henzinger et al 2006 Formats)

Model Key Features

Elie Bursztein
eb@lsv.ens-cachan.fr

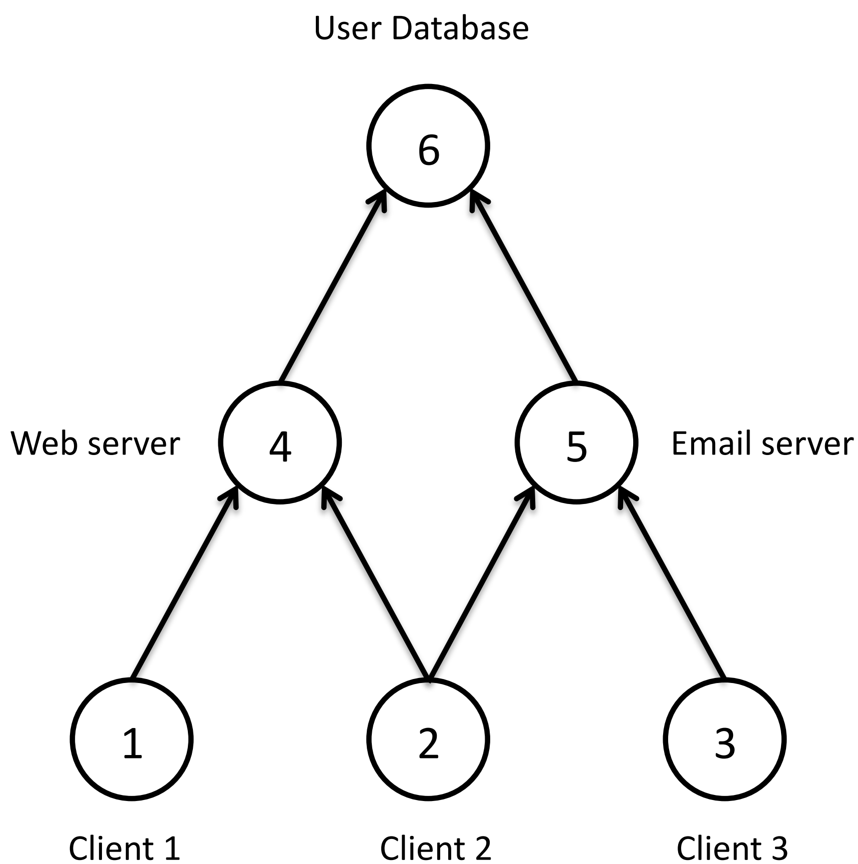
Dependency
- Collateral effects
- Trust relations

Interaction
- Administrator
- Intruder

Time
- Action take time

Dependency

Elie Bursztein
eb@lsv.ens-cachan.fr

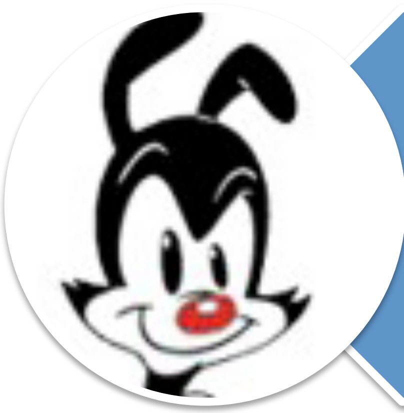


Network interaction

Elie Bursztein
eb@lsv.ens-cachan.fr

Exploit vulnerabilities

Abuse trust relations



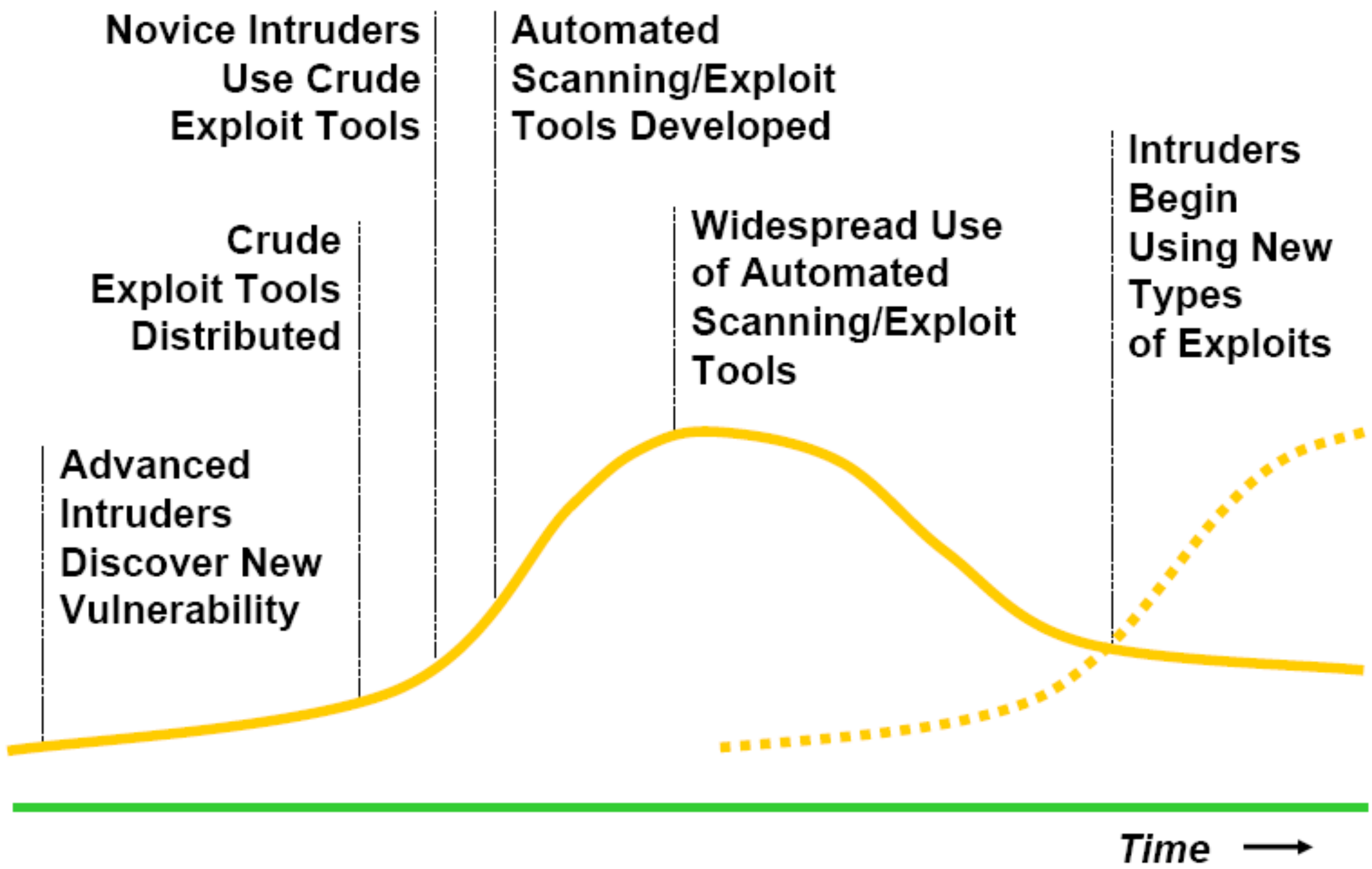
Patch

Firewall

Restore

Vulnerability cycle

Elie Bursztein
eb@lsv.ens-cachan.fr

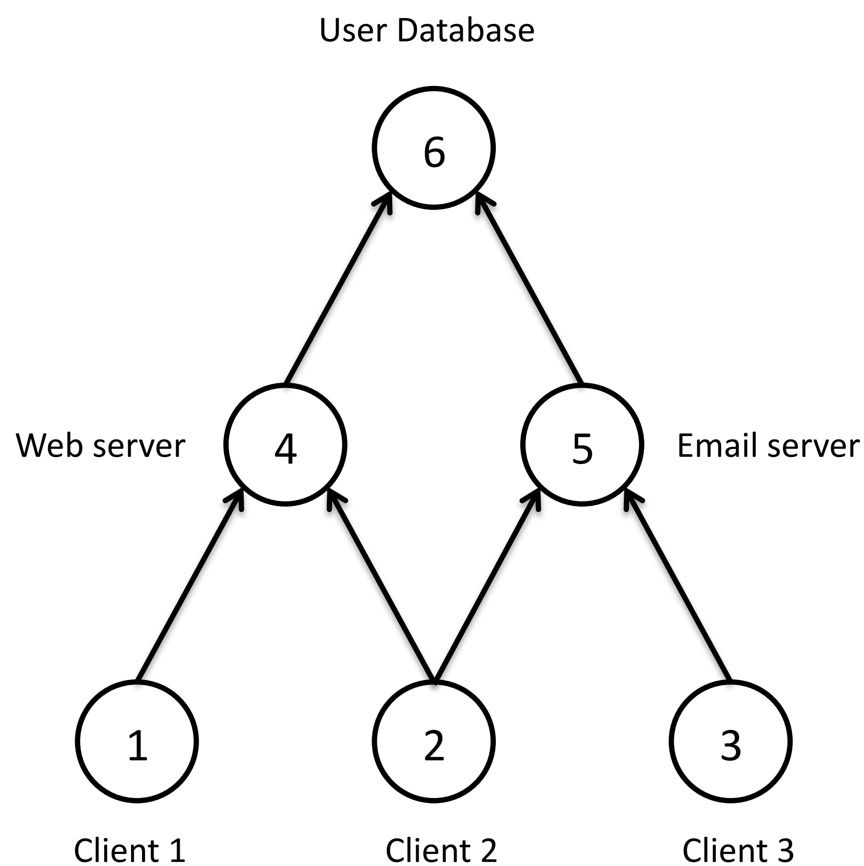


Cert/ Carnegie Mellon University

Network Information

Elie Bursztein
eb@lsv.ens-cachan.fr

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	⊥

Information Evolution

Elie Bursztein
eb@lsv.ens-cachan.fr

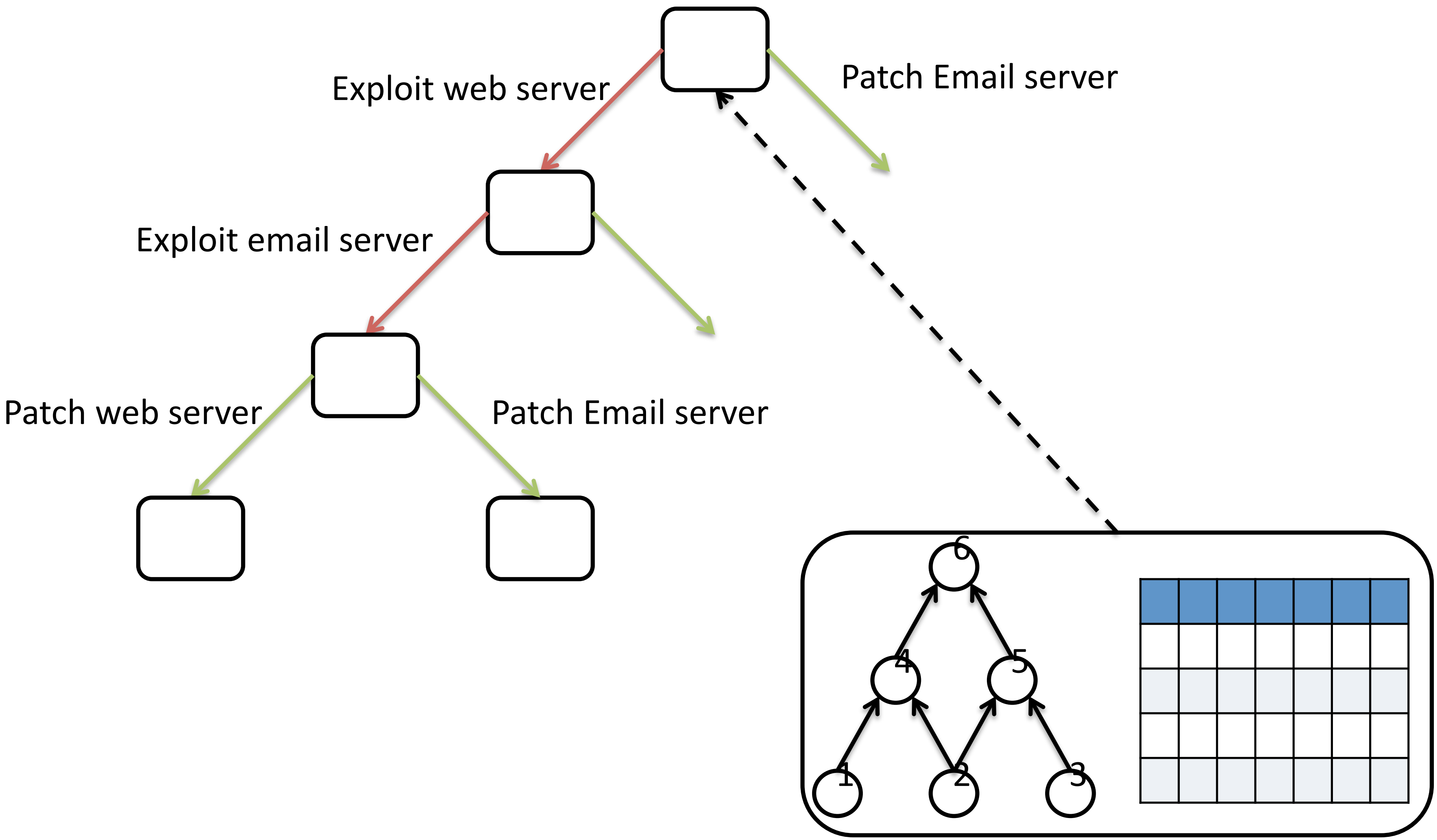
	1	2	3	4	5	6
ρ(Public)	⊥	⊥	⊥	T	T	⊥
ρ(Vuln)	⊥	⊥	⊥	T	T	⊥
ρ(Compr)	⊥	⊥	⊥	⊥	⊥	⊥
ρ(NeedPub)	⊥	⊥	⊥	T	T	⊥

Compr 4

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

A Incomplete Game Example

Elie Bursztein
eb@lsv.ens-cachan.fr



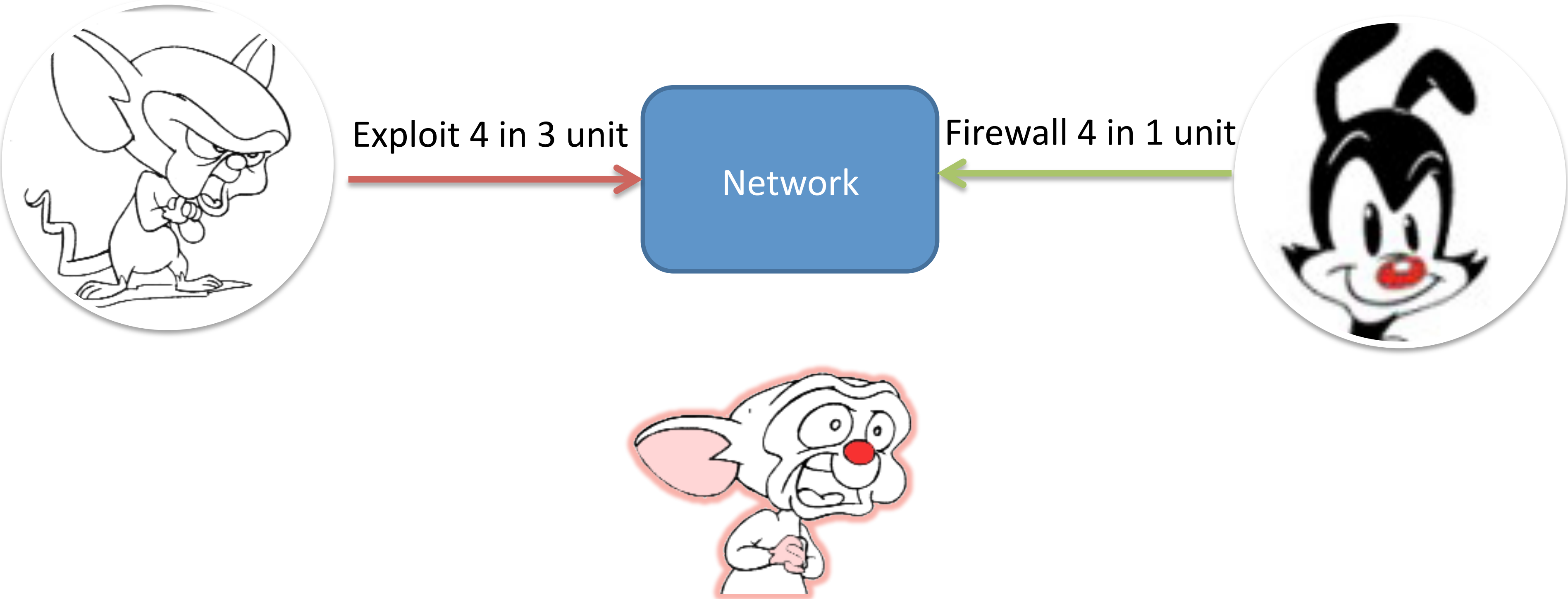
Time

Elie Bursztein
eb@lsv.ens-cachan.fr

- Each action requires a different amount of time
  - Patching a service: Download, extract, apply, restart
  - Exploit a service
  - Firewalling a service
- In anticipation games as in TATL the fastest action win
- Player can be taken by surprise

The element of surprise

Elie Bursztein
eb@lsv.ens-cachan.fr



Type of attacks

Elie Bursztein
eb@lsv.ens-cachan.fr

- Anticipation games allows to model
  - Denial of service
  - Buffer overflow execution
  - Permission abuse
  - Cross-scripting
  - Information leak
  - ….

Rule Language

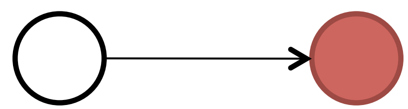
Elie Bursztein
eb@lsv.ens-cachan.fr

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

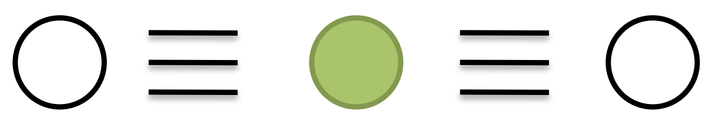
Semantic

Elie Bursztein
eb@lsv.ens-cachan.fr

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



$\vdash \Diamond_{\equiv} Public$ At least, one of the node the belongs to the equivalence is public



Rules example

Elie Bursztein
eb@lsv.ens-cachan.fr

$$\mathbf{Pre}\ Vuln \wedge Public \wedge \neg Compr \xrightarrow{(2,I,Compromise\ 0day)} Compr$$

$$\mathbf{Pre}\ Vuln \wedge Public \wedge \neg Compr \xrightarrow{(7,I,Compromise\ public)} Compr$$

$$\mathbf{Pre}\ \neg Compr \wedge \Diamond Compr \xrightarrow{(4,I,Compromise\ backward)} Compr$$

$$\mathbf{Pre}\ Compr \wedge \Diamond \neg Compr \xrightarrow{(4,I,Compromise\ forward)} \Diamond Compr$$

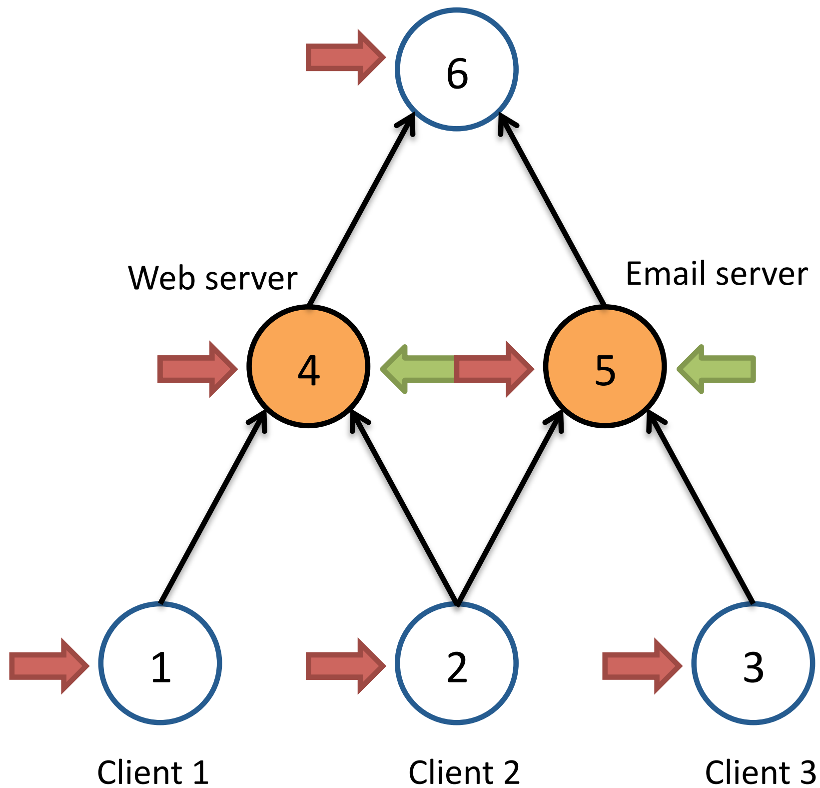
$$\mathbf{Pre}\ Public \wedge Vuln \xrightarrow{(1,A,Firewall)} \neg Public$$

$$\mathbf{Pre}\ Public \wedge \neg Vuln \wedge NeedPub \xrightarrow{(1,A,UnFirewall)} Public$$

$$\mathbf{Pre}\ Vuln \wedge \neg Compr \xrightarrow{(3,A,Patch)} \neg Vuln \wedge \neg Compr$$

A Play example

Elie Bursztein
eb@lsv.ens-cachan.fr



= [illegible]

Player	Action	Rule	Target	Succ
Admin	Execute	Firewall	4	
Intruder	Execute	Compromise Forward Backward	4	5

Properties Semantic

Elie Bursztein
eb@lsv.ens-cachan.fr

φ	$::=$	A	atomic propositions, in $\mathcal{A}$
	$\mid$	$\neg\varphi$	
	$\mid$	$\varphi \wedge \varphi$	
	$\mid$	$\Diamond\varphi$	
	$\mid$	$\Diamond_{\equiv}\varphi$	
	$\mid$	$x + d_1 \leq y + d_2$	clock constraints
	$\mid$	$x \cdot \varphi$	freeze
	$\mid$	$\langle\langle\mathfrak{P}\rangle\rangle\blacksquare\varphi$	invariant
	$\mid$	$\langle\langle\mathfrak{P}\rangle\rangle\varphi_1 \; \mathcal{U} \; \varphi_2$	eventually

We abbreviate $\langle\langle\mathfrak{P}\rangle\rangle \text{TRUE} \; \mathcal{U} \; \varphi$ as $\langle\langle\mathfrak{P}\rangle\rangle\blacklozenge\varphi$.

Semantic

Elie Bursztein
eb@lsv.ens-cachan.fr

$\vdash \langle\langle A \rangle\rangle \varphi$ The player A have a strategy to satisfy the property φ

$\vdash \blacksquare Compr$ In every future the node will be compromised

Properties Illustration

Elie Bursztein
eb@lsv.ens-cachan.fr

$$\langle\!\langle \mathsf{A} \rangle\!\rangle \blacksquare \Diamond_{\equiv} \neg \mathsf{Compr}$$

$$\langle\!\langle \mathsf{A} \rangle\!\rangle \blacksquare x \cdot \neg \Diamond_{\equiv} \mathsf{Avail} \Rightarrow [\langle\!\langle \mathsf{A} \rangle\!\rangle \blacklozenge y \cdot y \leq x + d \wedge \langle\!\langle \mathsf{A} \rangle\!\rangle \blacksquare z \cdot z \leq y + d' \Rightarrow \Diamond_{\equiv} \mathsf{Avail}]$$

Decidability

Elie Bursztein
eb@lsv.ens-cachan.fr

Anticipation game are EXPTIME-complete

Elie Bursztein
eb@lsv.ens-cachan.fr

One More Thing !

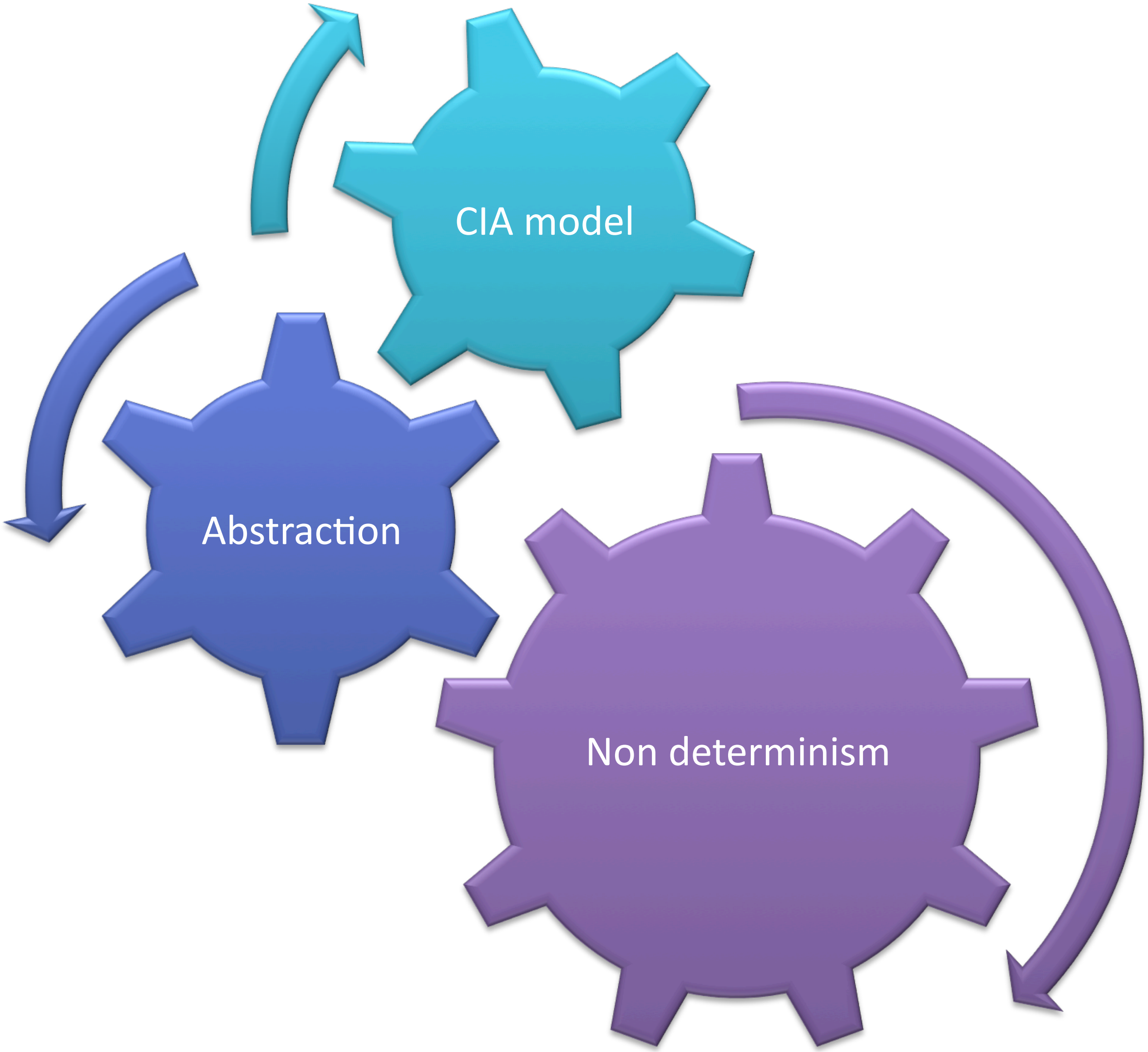
It Work!

Elie Bursztein
eb@lsv.ens-cachan.fr

- Model and Strategies are fully implemented in C
- The talk example cannot be analyzed by hand
  - 4011 plays
  - 40825 states

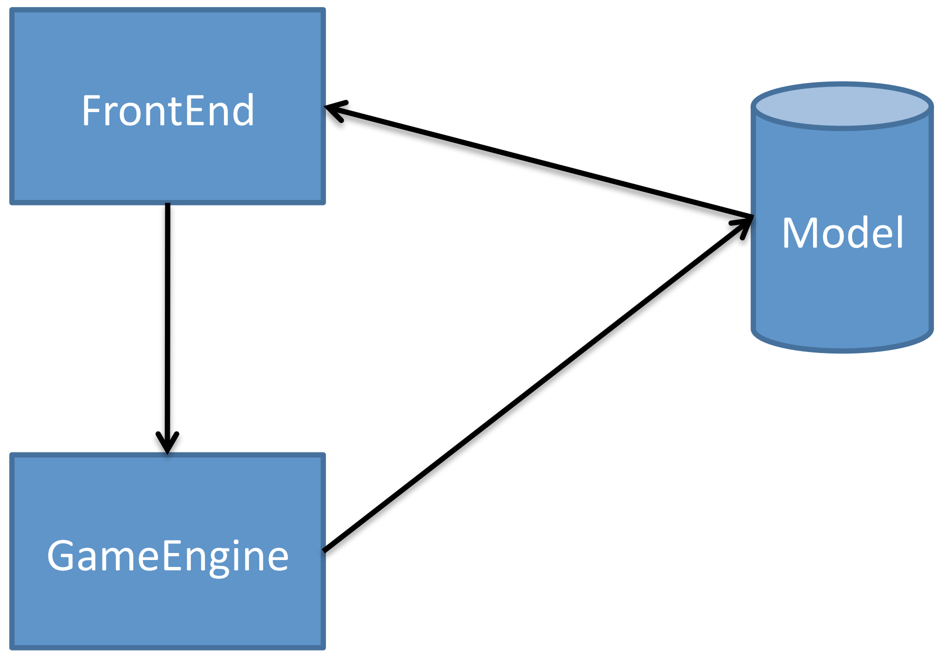
Future Work

Elie Bursztein
eb@lsv.ens-cachan.fr



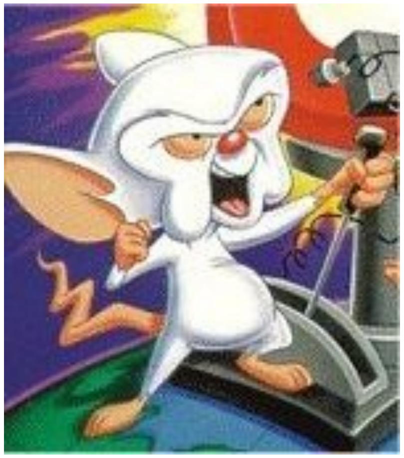
The framework

Elie Bursztein
eb@lsv.ens-cachan.fr



Elie Bursztein
eb@lsv.ens-cachan.fr

Analyzer Demo



Conclusion

Elie Bursztein
eb@lsv.ens-cachan.fr

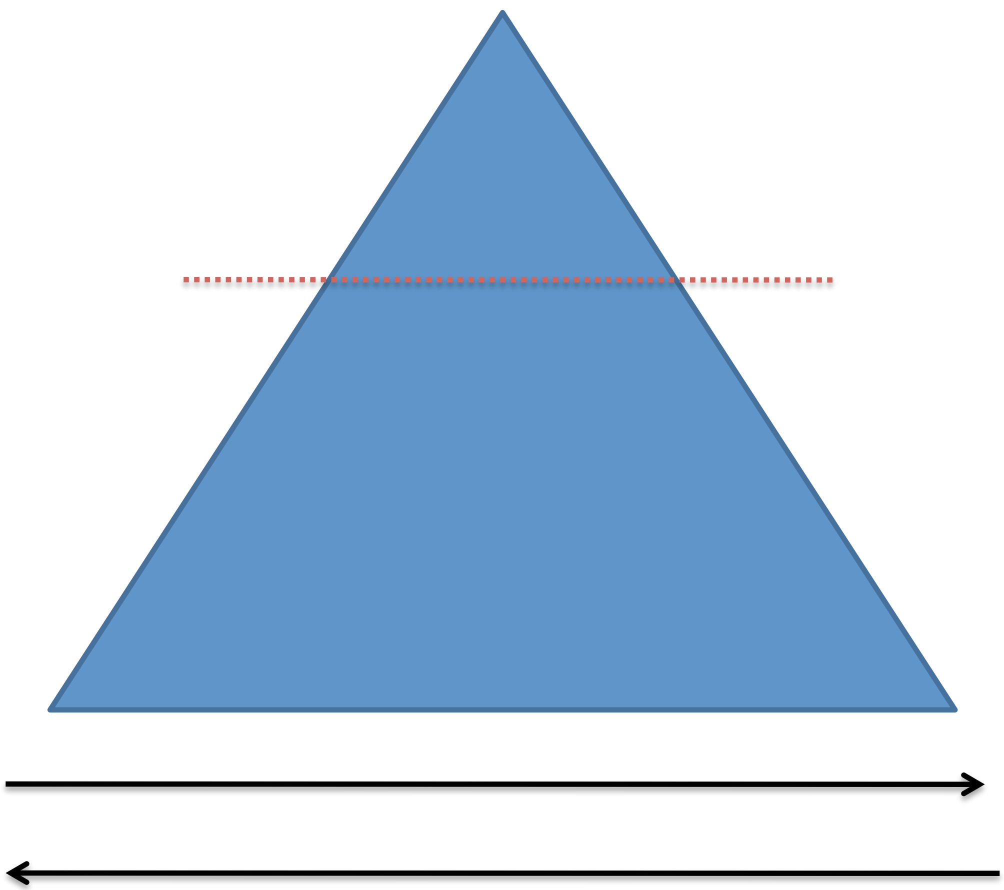
- Game and Time provide a richer model for intrusion analysis
- Many directions to explore

Questions

Elie Bursztein
eb@lsv.ens-cachan.fr

During this work no network service was injured or tortured.

Elie Bursztein
eb@lsv.ens-cachan.fr



Rule execution time