A Logical Framework for Anticipation of Network Incidents

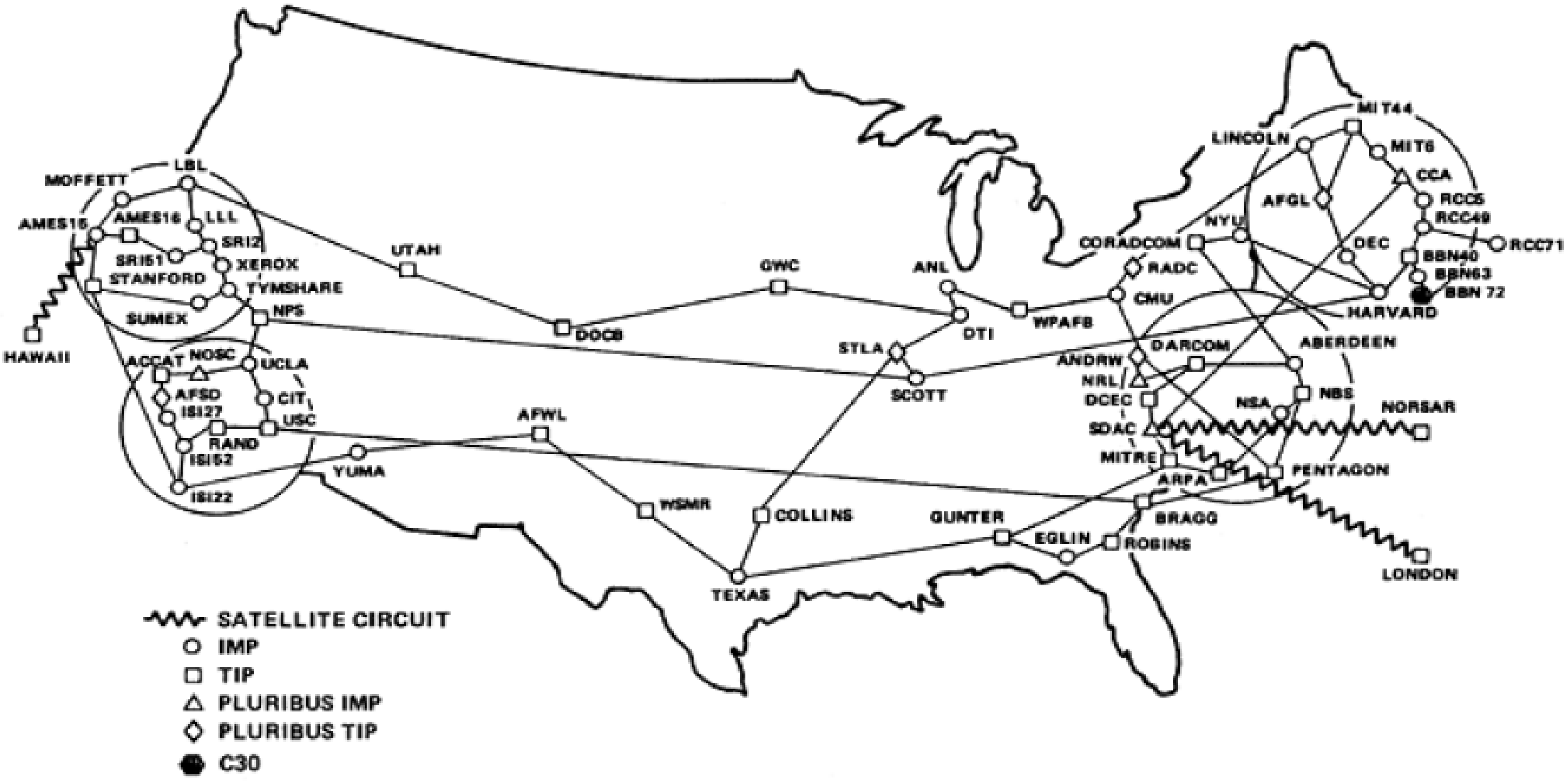
Elie Bursztein and Jean Goubault-Larrecq
Phd Student LSV ENS-CACHAN CNRS INRIA DGA

Outline

- 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

ARPANET GEOGRAPHIC MAP, OCTOBER 1980

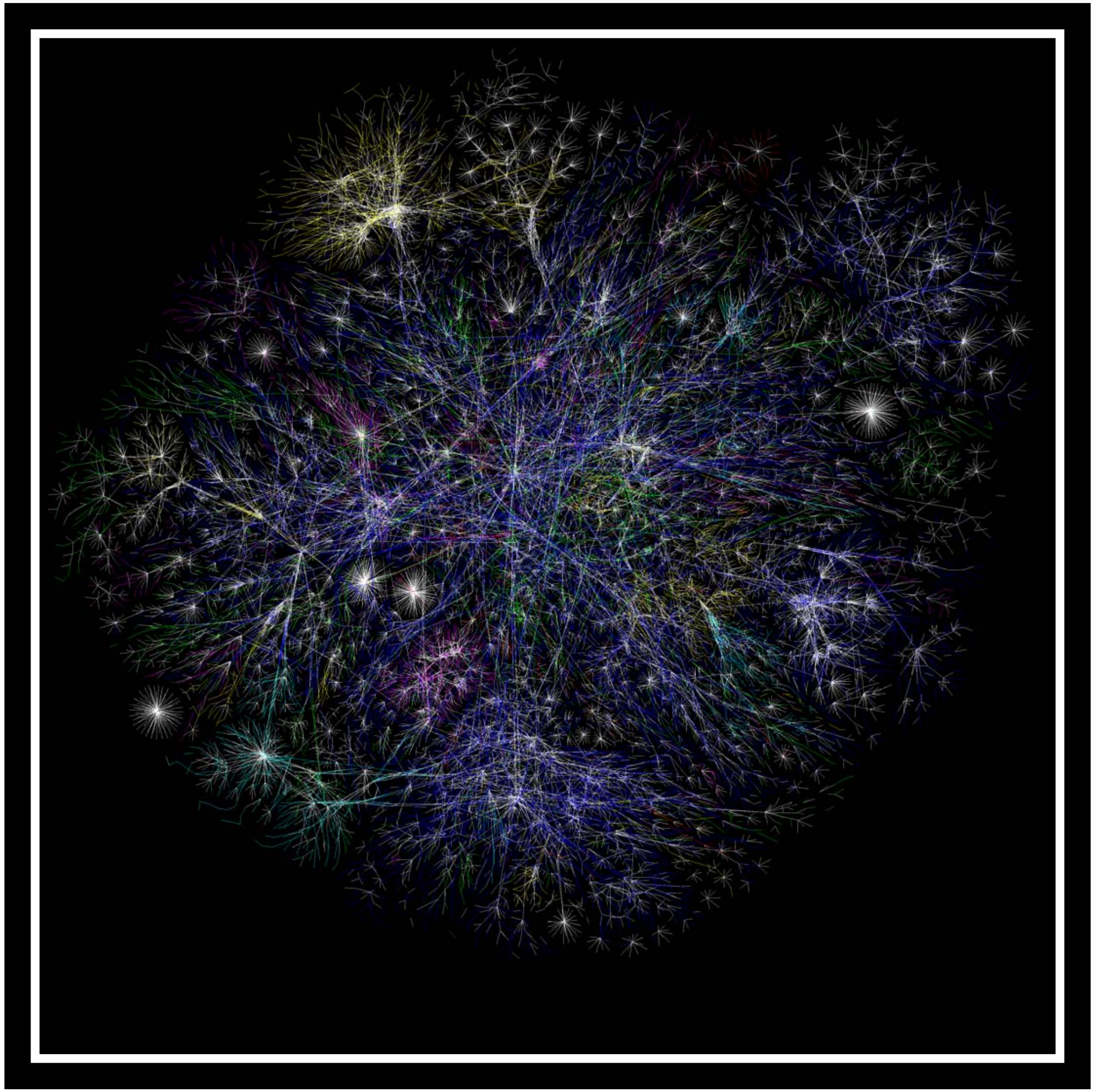


SATELLITE CIRCUIT
○ IMP
□ TIP
△ PLURIBUS IMP
◇ PLURIBUS TIP
● C30

(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

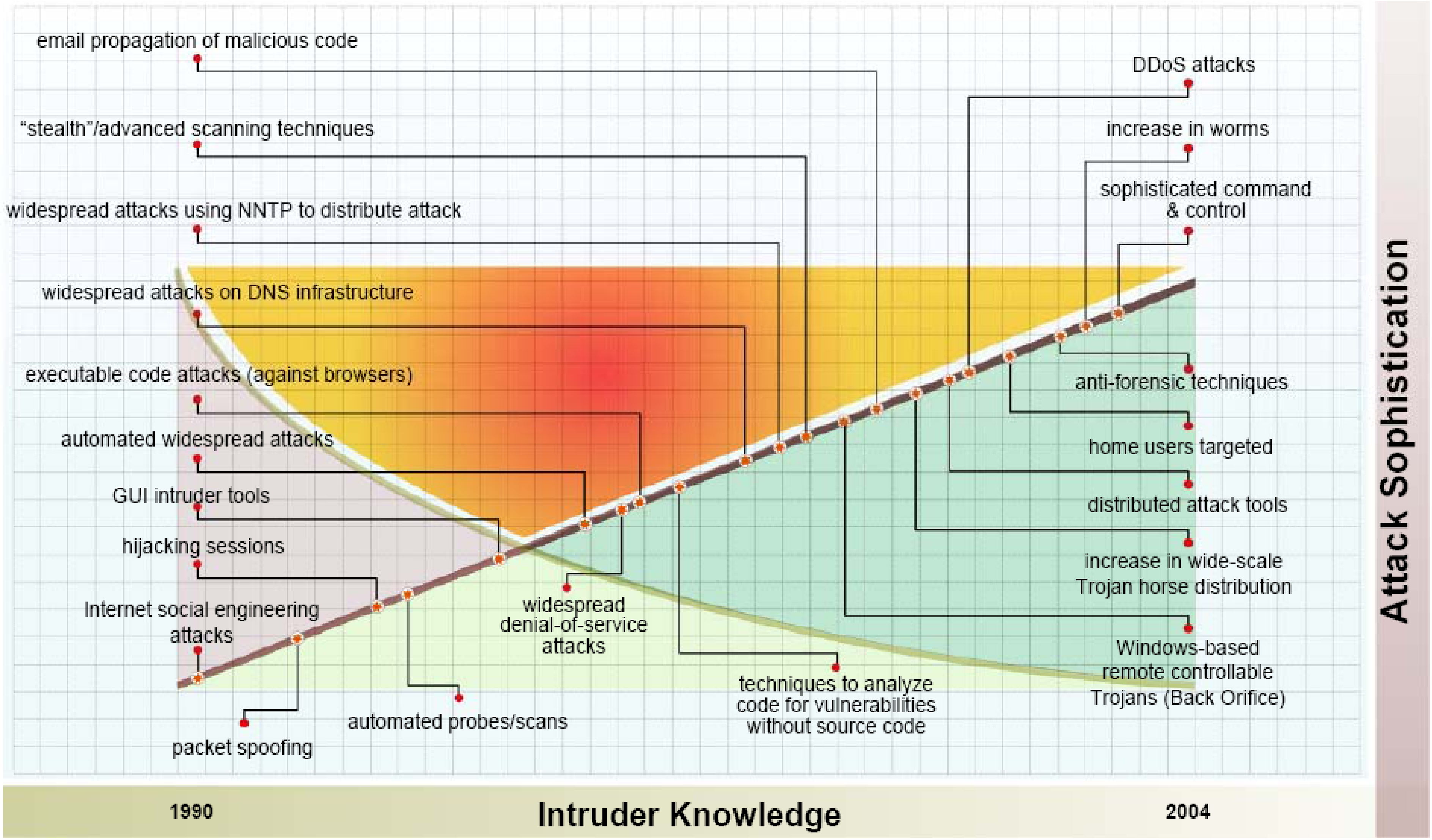
The Current Internet

Elie Bursztein
eb@lsv.ens-cachan.fr



Opte project

Attack Sophistication vs. Intruder Knowledge



Cert/ Carnegie Mellon University

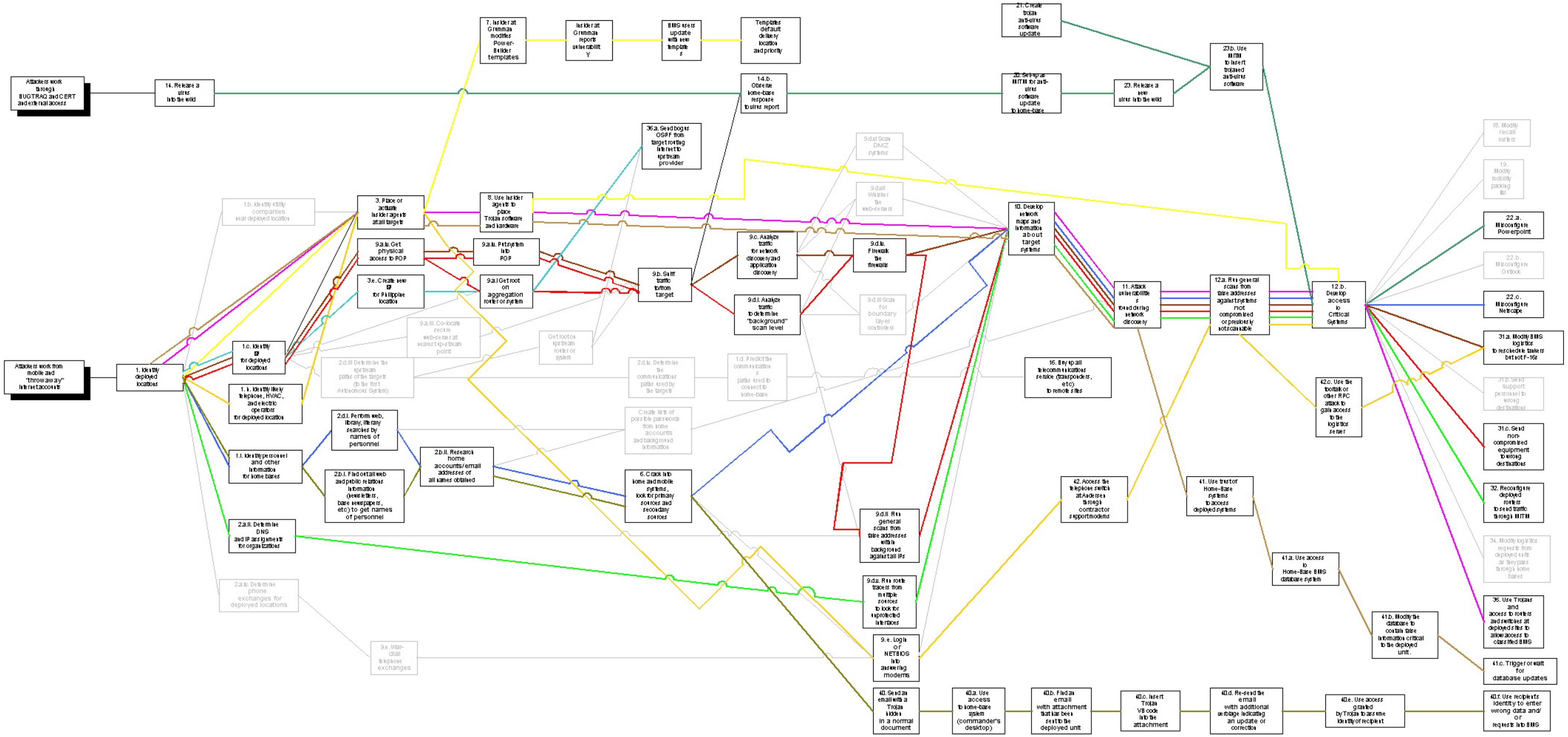
Attack Step-stones

- 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

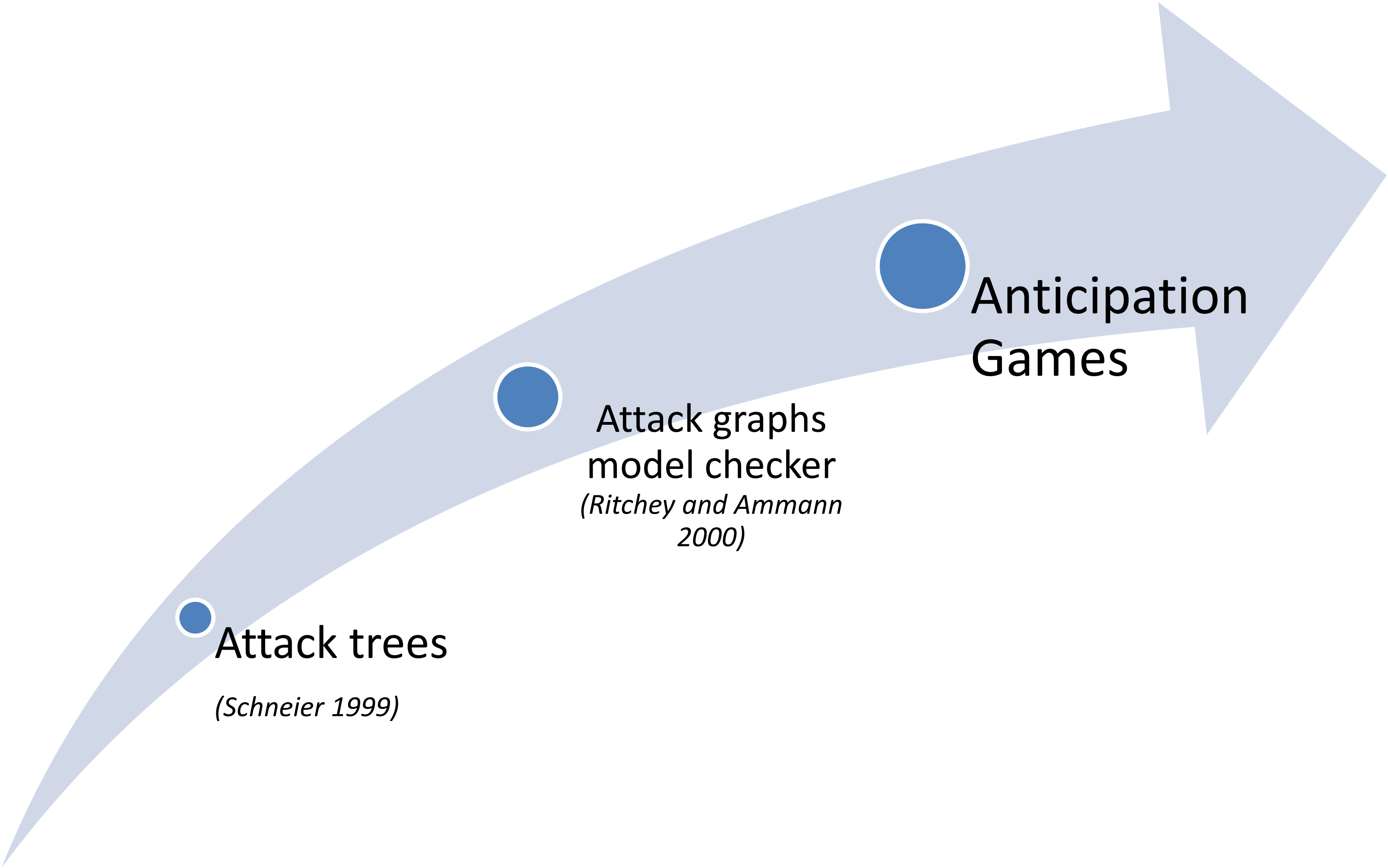
Attack Graph Example

Elie Bursztein
eb@lsv.ens-cachan.fr


Attackers work through BUGTRAQ and CERT and external access
14. Release a virus into the wild
7. Insider at Grumman modifies Power-Builder templates
Insider at Grumman reports vulnerability
BMS users update with new templates
Templates default delivery location and priority
14.b. Observe home-base response to virus report
21. Create trojan anti-virus software update
20. Set-up as MITM for anti-virus software update to home-base
23. Release a new virus into the wild
23.b. Use MITM to insert trojaned anti-virus software
36.a. Send bogus OSPF from target routing Internet to upstream provider
9.d.I Scan DMZ systems
9.d.II Whisker the web-servers
1.b. Identify utility companies near deployed locations
3. Place or activate insider agents at all targets
8. Use insider agents to place Trojan software and hardware
9.a.ii. Get physical access to POP
9.a.ii. Put system into POP
3.e. Create new ISP for Philippine location
9.a.I Get root on aggregation router or system
9.b. Sniff traffic to/from target
9.c. Analyze traffic for network discovery and application discovery
9.d.ii. Firewalk the firewalls
9.d.I. Analyze traffic to determine "background" scan level
9.d.III Scan for boundary layer controllers
10. Develop network maps and information about target systems
11. Attack vulnerabilities found during network discovery
12a. Run general scans from false addresses against systems not compromised or previously not scannable
12.b. Develop access to Critical Systems
18. Modify recall rosters
19. Modify mobility packing list
22.a. Misconfigure Powerpoint
22.b. Misconfigure Outlook
22.c. Misconfigure Netscape
31.a. Modify BMS logistics to reschedule tankers but not F-16s
31.b. Send support personnel to wrong destinations
31.c. Send non-compromised equipment to wrong destinations
32. Reconfigure deployed routers to send traffic through MITM
34. Modify logistics requests from deployed units as they pass through home bases
35. Use Trojans and access to routers and switches at deployed sites to allow access to classified BMS
9.a.III. Co-locate secure web-server at nearest up-stream point
Get root on upstream router or system
2.d.III Determine the upstream paths of the targets (to the first Autonomous System)
2.d.ii. Determine the communications paths used by the targets
1.d. Predict the communications paths used to connect to home-base
16. Buy up all telecommunications service (transponders, etc) to remote sites
42.c. Use the tooltalk or other RPC attack to gain access to the logistics server
Attackers work from mobile and "throw away" Internet accounts
1. Identify deployed locations
1.c. Identify ISP for deployed locations
1.ii. Identify likely telephone, HVAC, and electric operators for deployed location
1.i. Identify personnel and other information for home bases
2.d.I. Perform web, library, literary searches by names of personnel
2.b.I. Find out all web and public relations information (newsletters, base newspapers, etc) to get names of personnel
2.b.II. Research home accounts/email addresses of all names obtained
Create lists of possible passwords from home accounts and background information
6. Crack into home and mobile systems, look for primary sources and secondary sources
2.a.II. Determine DNS and IP assignments for organizations
2.a.ii. Determine phone exchanges for deployed locations
9.e. War-dial telephone exchanges
9.d.II Run general scans from false addresses within background against all IPs
9.d.ii. Run route tracers from multiple sources to look for unprotected interfaces
9.e. Login or NETBIOS into answering modems
42. Access the telephone switch at Andersen through contractor support modems
41. Use trust of Home-Base systems to access deployed systems
41.a. Use access to Home-Base BMS database system
41.b. Modify the database to contain false information critical to the deployed unit.
41.c. Trigger or wait for database updates
40. Send an email with a Trojan hidden in a normal document
40.a. Use access to home-base system (commander's desktop)
40.b. Find an email with attachment that has been sent to the deployed unit
40.c. Insert Trojan VB code into the attachment
40.d. Re-send the email with additional verbiage indicating an update or correction
40.e. Use access granted by Trojan to assume identity of recipient
40.f. Use recipients identity to enter wrong data and/or requests into BMS

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

Model Evolution



Attack trees

(Schneier 1999)

Attack graphs model checker

(Ritchey and Ammann 2000)

Anticipation Games

Related Work

- 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

Dependency

- Collateral effects
- Trust relations

Interaction

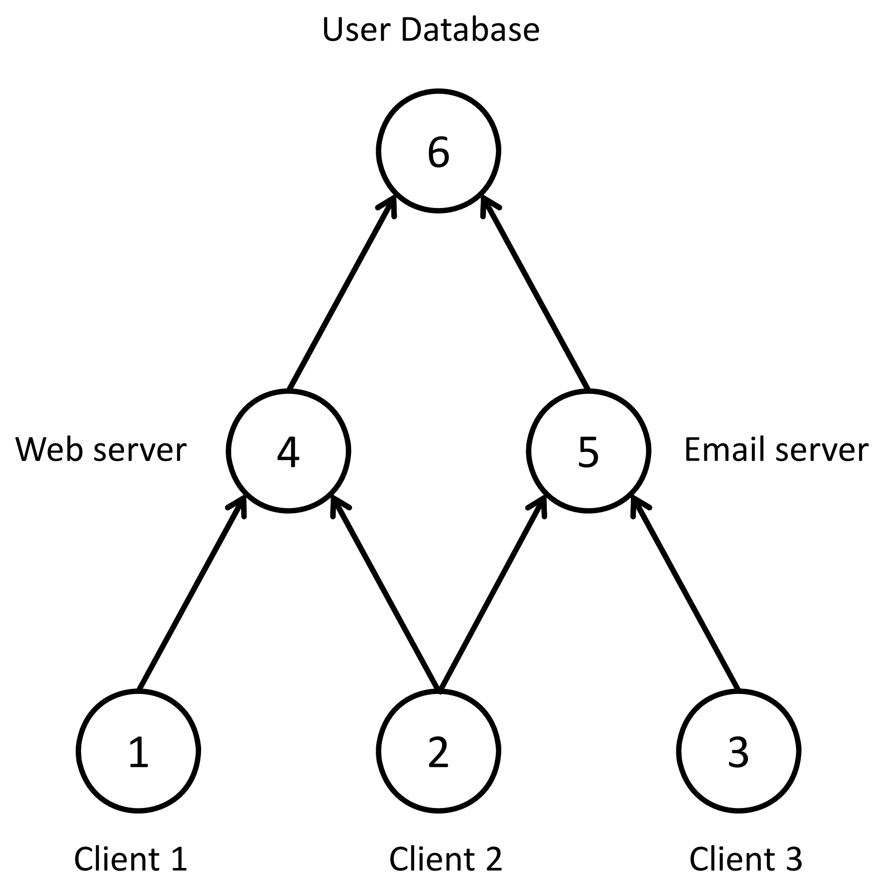
- Administrator
- Intruder

Time

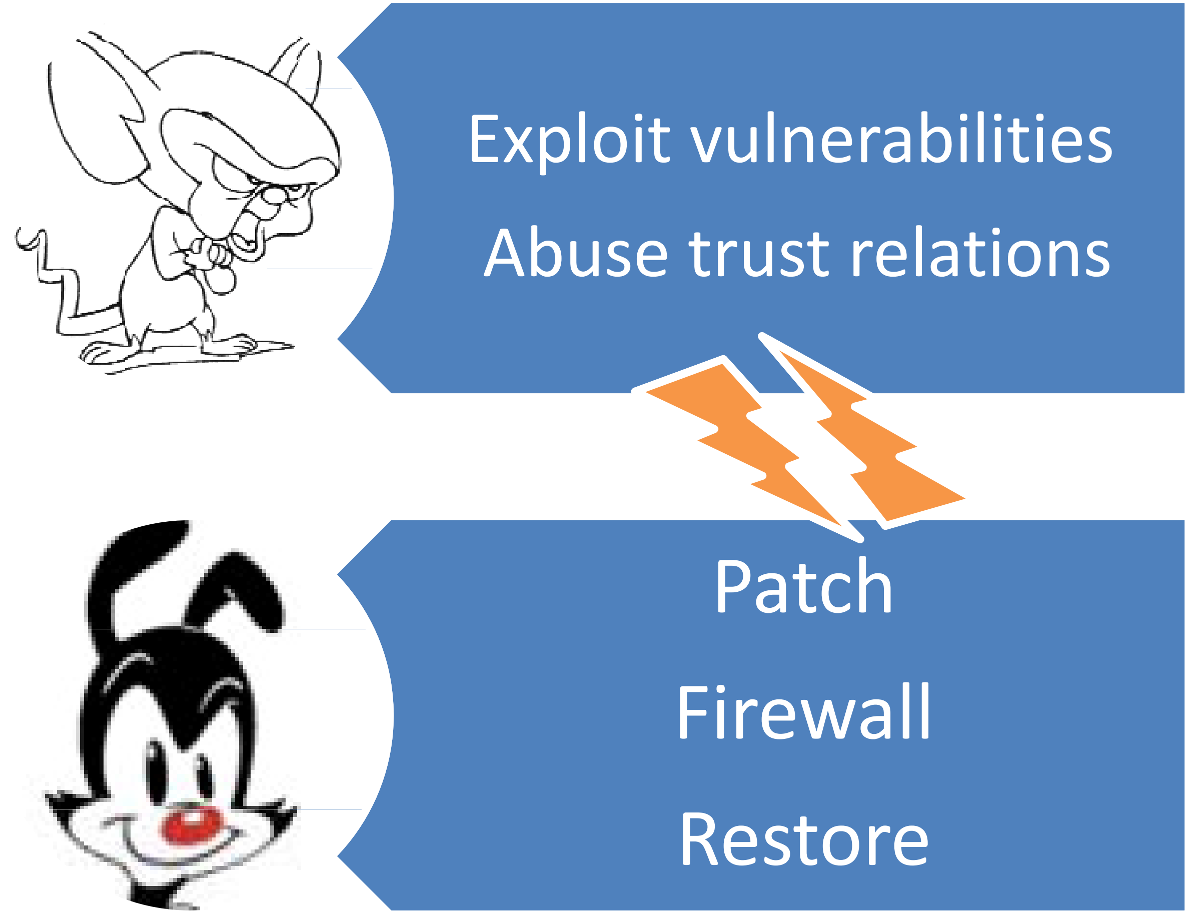
- Action take time

Dependency

Elie Bursztein
eb@lsv.ens-cachan.fr



Network interaction



Exploit vulnerabilities

Abuse trust relations

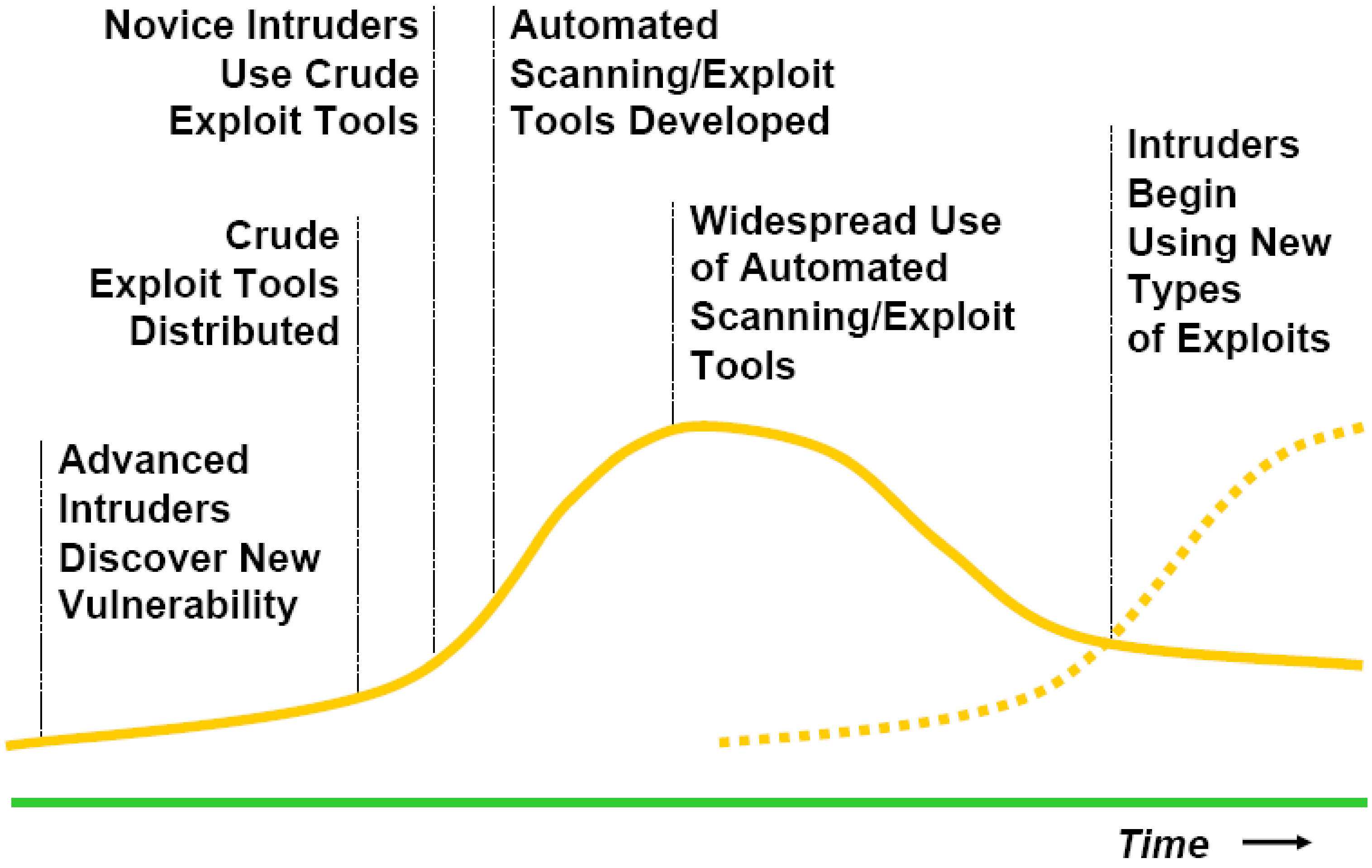
Patch

Firewall

Restore

Vulnerability cycle

Elie Bursztein
eb@lsv.ens-cachan.fr

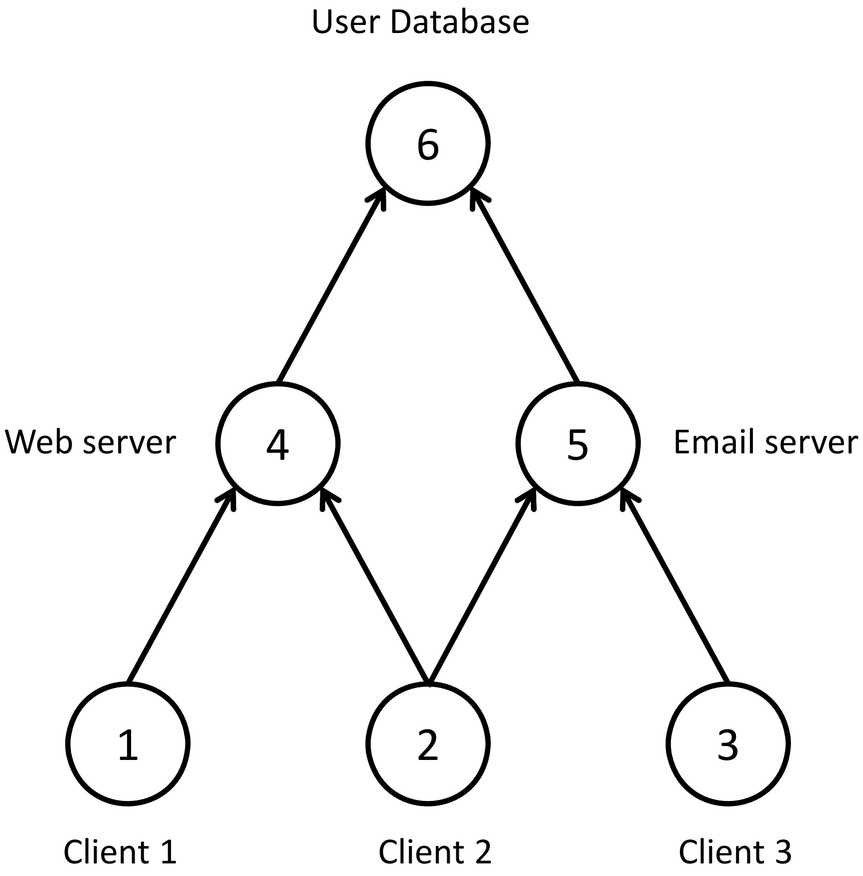


Cert/ Carnegie Mellon University

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

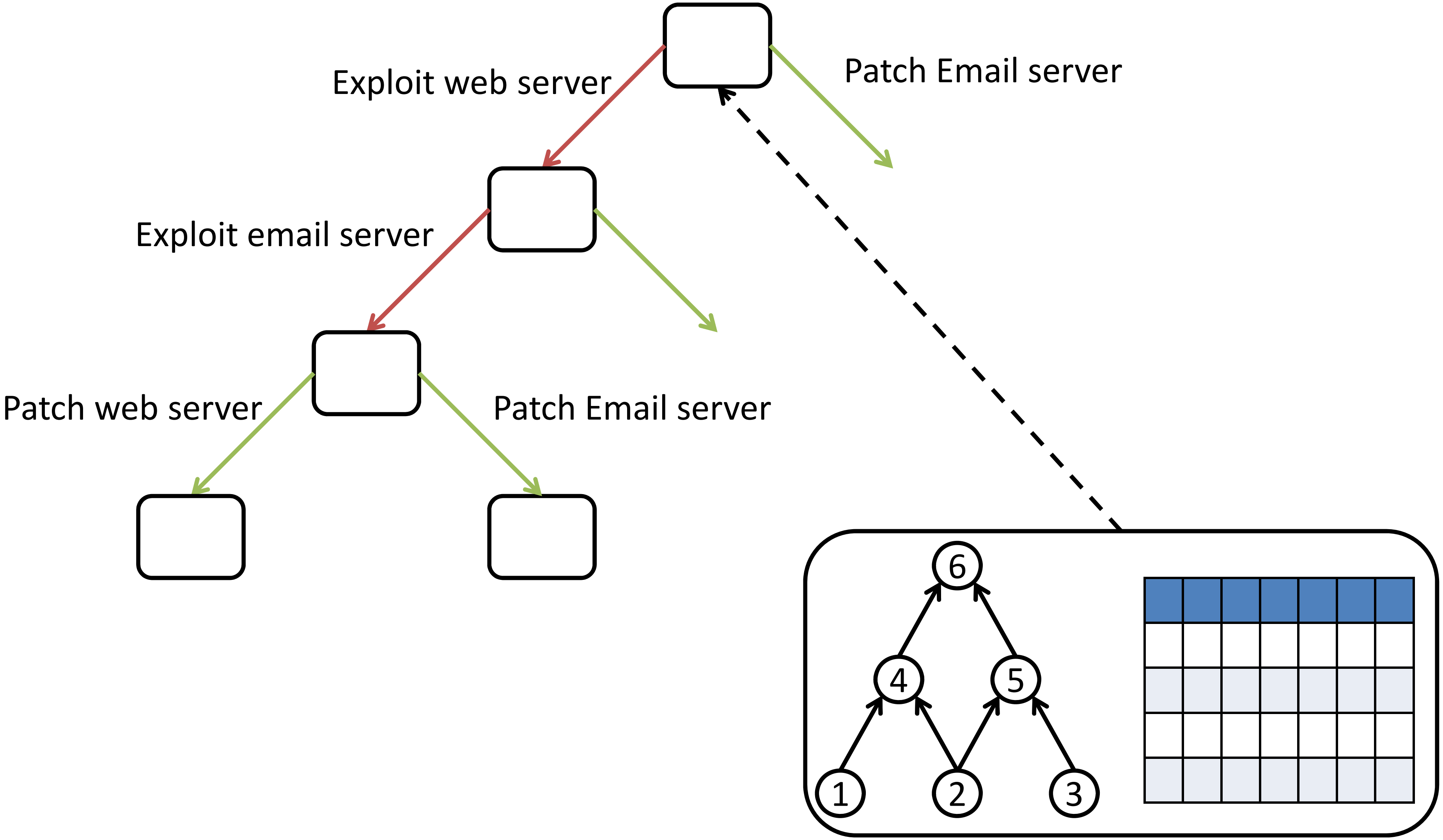
	1	2	3	4	5	6
ρ(Public)	⊥	⊥	⊥	T	T	⊥
ρ(Vuln)	⊥	⊥	⊥	T	T	⊥
ρ(Compr)	⊥	⊥	⊥	⊥	⊥	⊥
ρ(NeedPub)	⊥	⊥	⊥	T	T	⊥

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

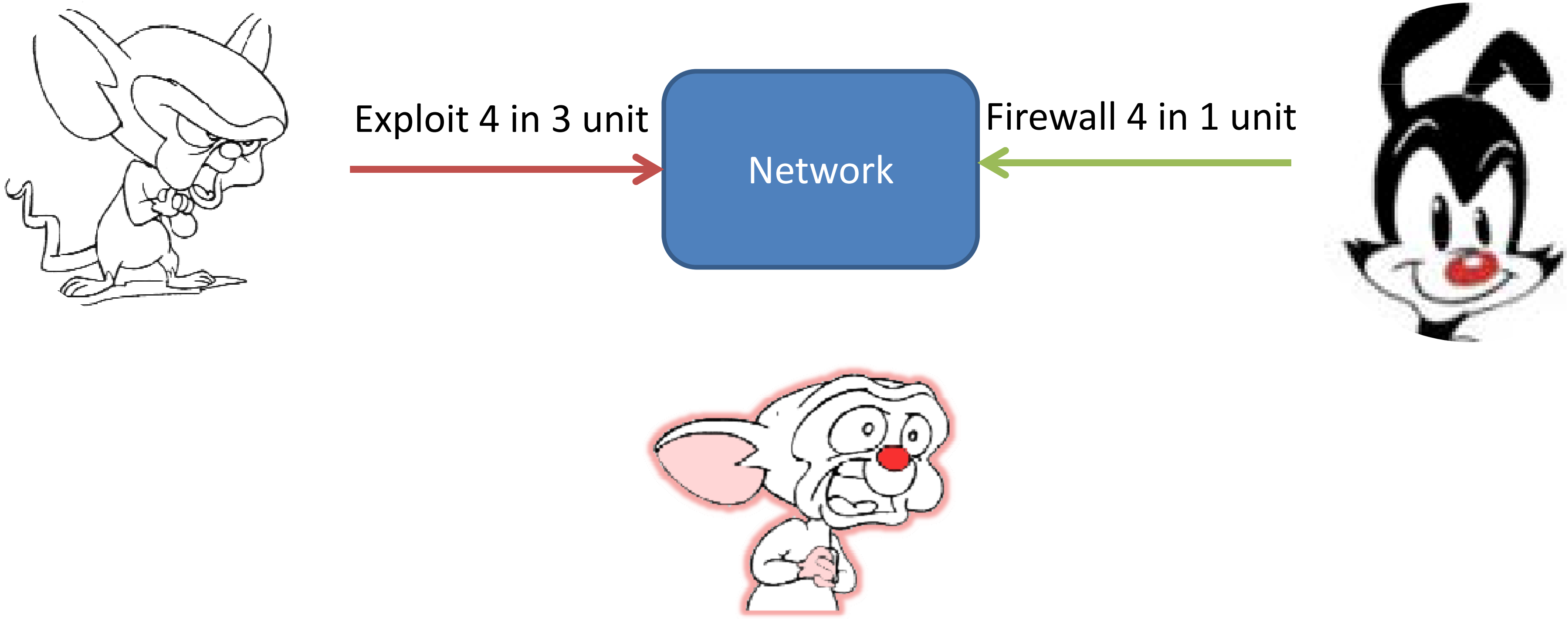
Elie Bursztein
eb@lsv.ens-cachan.fr



Time

- 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



Exploit 4 in 3 unit

Network

Firewall 4 in 1 unit

Type of attacks

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

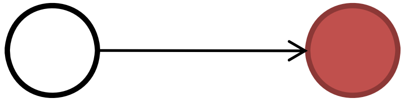
Rule Language

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

Semantic

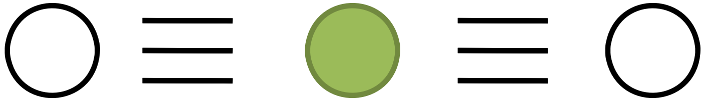
$\vdash \Diamond Compr$

A successor node is compromised



$\vdash \Diamond_{\equiv} Public$

At least, one of the node the belongs to the equivalence is public

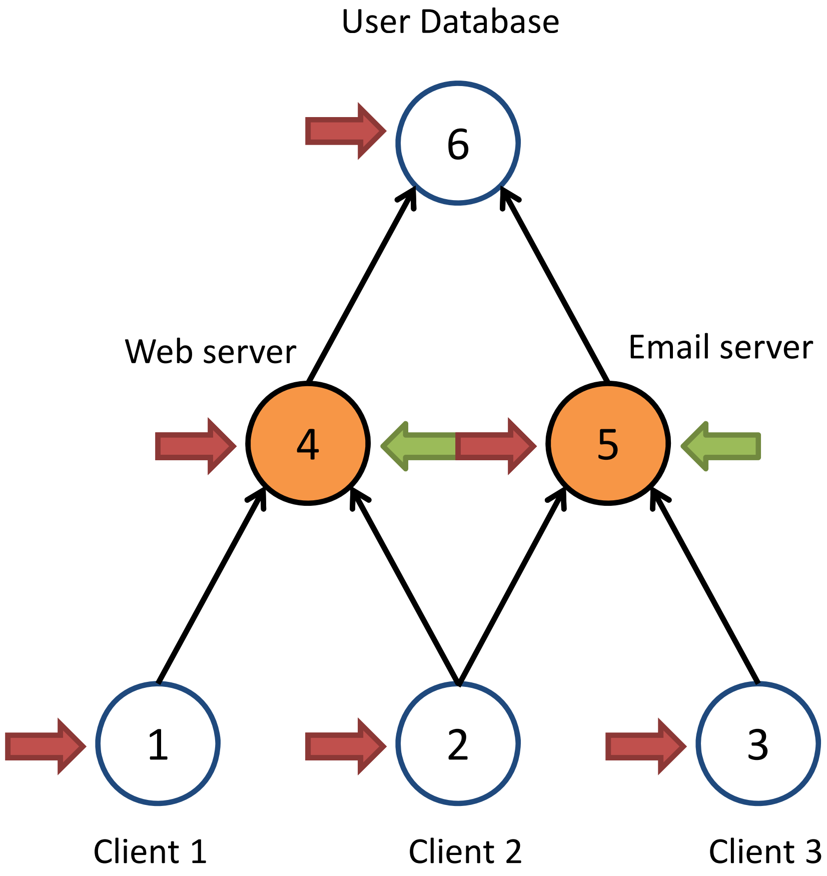


Rules example

$$\begin{aligned}
\textbf{Pre}\ Vuln \wedge Public \wedge \neg Compr &\xrightarrow{(2,I,Compromise\ 0day)} Compr\\
\textbf{Pre}\ Vuln \wedge Public \wedge \neg Compr &\xrightarrow{(7,I,Compromise\ public)} Compr\\
\textbf{Pre}\ \neg Compr \wedge \Diamond Compr &\xrightarrow{(4,I,Compromise\ backward)} Compr\\
\textbf{Pre}\ Compr \wedge \Diamond \neg Compr &\xrightarrow{(4,I,Compromise\ forward)} \Diamond Compr\\
\textbf{Pre}\ Public \wedge Vuln &\xrightarrow{(1,A,Firewall)} \neg Public\\
\textbf{Pre}\ Public \wedge \neg Vuln \wedge NeedPub &\xrightarrow{(1,A,UnFirewall)} Public\\
\textbf{Pre}\ Vuln \wedge \neg Compr &\xrightarrow{(3,A,Patch)} \neg Vuln \wedge \neg Compr
\end{aligned}$$

A Play example

Elie Bursztein
eb@lsv.ens-cachan.fr



= 30

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

Properties Semantic

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

We abbreviate $\langle\!\langle \mathfrak{P} \rangle\!\rangle \mathrm{TRUE} \, \mathcal{U} \, \varphi$ as $\langle\!\langle \mathfrak{P} \rangle\!\rangle \blacklozenge \varphi$.

Semantic

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

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

Property Illustration

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

Decidability

TATL Formula model checking in Anticipation game is decidable and EXPTIME-complete

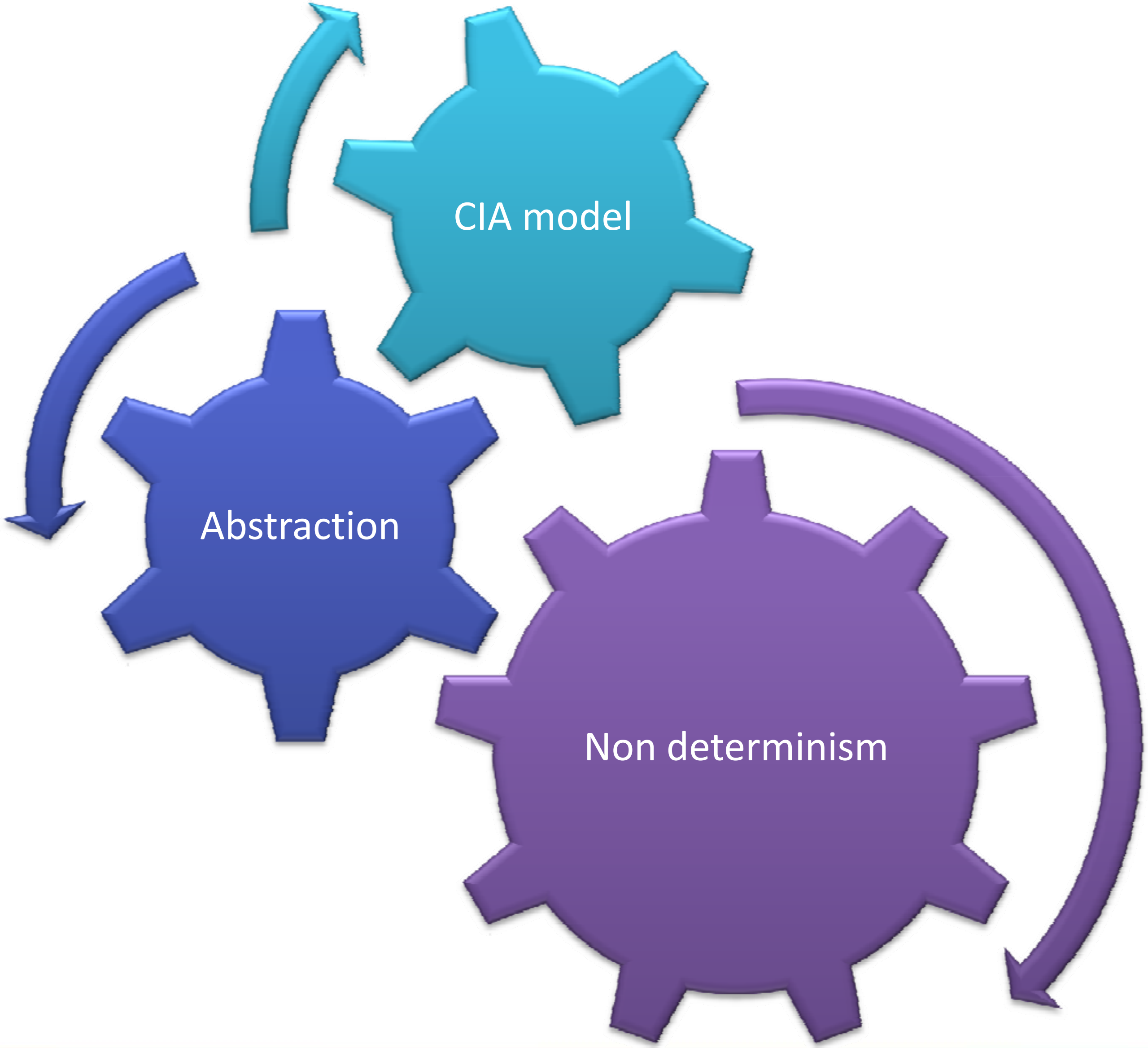
One More Thing !

It Work!

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

Analyzer Demo

Future Work

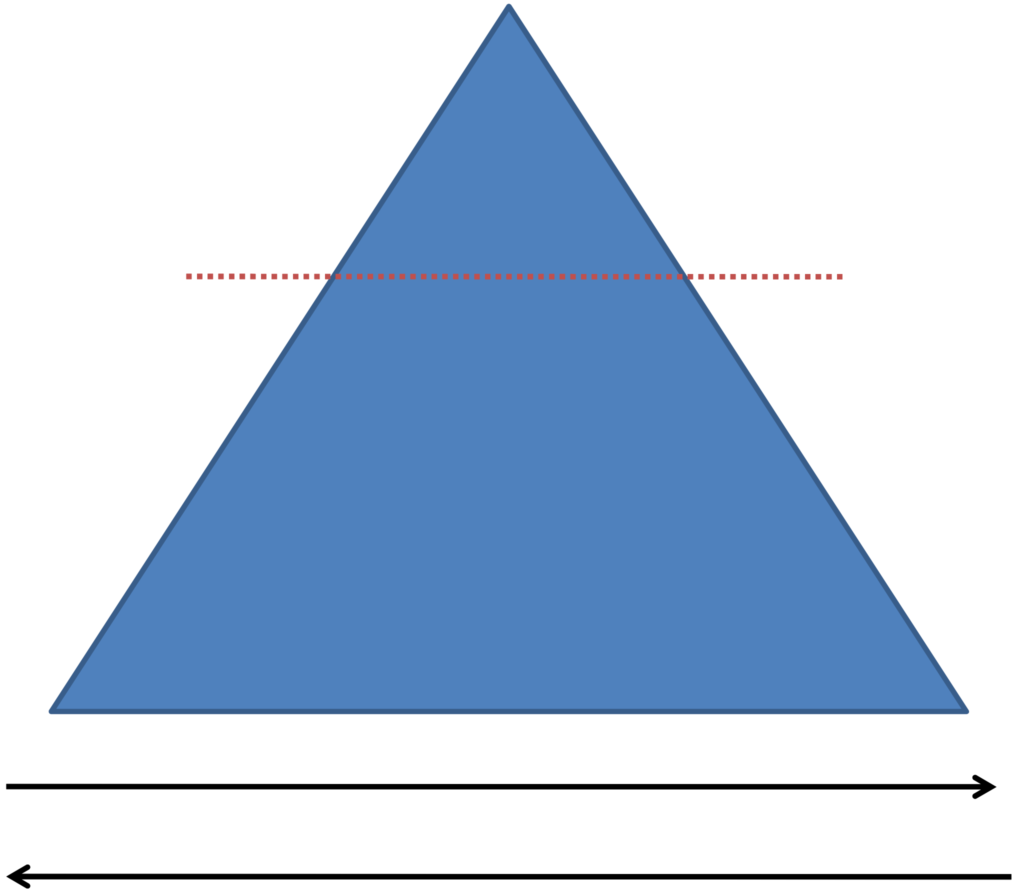


Conclusion

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

Questions

During this work no network service was injured or tortured.



Rule execution time