Anticipation Games

Elie Bursztein
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

Outline:

Introduction > Model > Strategy > Conclusion
The Current Internet

Opte project
A Logical Framework for Evaluating Network Resilience Against Faults

Elie Bursztein
eb@lsv.ens-cachan.fr

Outline:
- Introduction
- Model
- Strategy
- Conclusion

Cert/ Carnegie Mellon University

28/11/2007
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
Outline:

- Introduction
- Model
- Strategy
- Conclusion

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

28/11/2007
A Logical Framework for Evaluating Network Resilience Against Faults

Outline:
1. Introduction
2. Model
3. Strategy
4. Conclusion

- Attack trees (Schneier 1999)
- Attack graphs (Ritchey and Ammann 2000)
- Anticipation Games
- Model Evolution

Elie Bursztein
eb@lsv.ens-cachan.fr
28/11/2007
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
A Logical Framework for Evaluating Network Resilience Against Faults

Elie Bursztein
eb@lsv.ens-cachan.fr

Outline:
- Introduction
- Model
- Strategy
- Conclusion

Client 1

Web server

Client 2

User Database

Client 3

Email server

28/11/2007

Outline: Introduction > Model > Strategy > Conclusion
A Logical Framework for Evaluating Network Resilience Against Faults

Elie Bursztein
 eb@lsv.ens-cachan.fr

Outline:
- Introduction
- Model
- Strategy
- Conclusion

28/11/2007

Network interaction

Exploit vulnerabilities
Abuse trust relations

Patch
Firewall
Restore
A Logical Framework for Evaluating Network Resilience Against Faults

Elie Bursztein
eb@lsv.ens-cachan.fr

Outline:

- Introduction
- Model
- Strategy
- Conclusion

Cert/ Carnegie Mellon University

28/11/2007
A Logical Framework for Evaluating Network Resilience Against Faults

Elie Bursztein
eb@lsv.ens-cachan.fr

Outline:
- Introduction
- Model
- Strategy
- Conclusion

Network Information

Fixed over the time

Evolve over time

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \rho(\text{Public}) )</td>
<td>( \perp )</td>
<td>( \perp )</td>
<td>( \perp )</td>
<td>( \top )</td>
<td>( \top )</td>
<td>( \perp )</td>
</tr>
<tr>
<td>( \rho(\text{Vuln}) )</td>
<td>( \perp )</td>
<td>( \perp )</td>
<td>( \perp )</td>
<td>( \top )</td>
<td>( \top )</td>
<td>( \perp )</td>
</tr>
<tr>
<td>( \rho(\text{Compr}) )</td>
<td>( \perp )</td>
<td>( \perp )</td>
<td>( \perp )</td>
<td>( \perp )</td>
<td>( \perp )</td>
<td>( \perp )</td>
</tr>
<tr>
<td>( \rho(\text{NeedPub}) )</td>
<td>( \perp )</td>
<td>( \perp )</td>
<td>( \perp )</td>
<td>( \top )</td>
<td>( \top )</td>
<td>( \perp )</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>----------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>( \rho ) (Public)</td>
<td>\bot</td>
<td>\bot</td>
<td>T</td>
<td>T</td>
<td>\bot</td>
<td></td>
</tr>
<tr>
<td>( \rho ) (Vuln)</td>
<td>\bot</td>
<td>\bot</td>
<td>T</td>
<td>T</td>
<td>\bot</td>
<td></td>
</tr>
<tr>
<td>( \rho ) (Compr)</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
</tr>
<tr>
<td>( \rho ) (NeedPub)</td>
<td>\bot</td>
<td>\bot</td>
<td>T</td>
<td>T</td>
<td>\bot</td>
<td></td>
</tr>
</tbody>
</table>

Compr 4

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \rho ) (Public)</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>T</td>
<td>T</td>
<td>\bot</td>
</tr>
<tr>
<td>( \rho ) (Vuln)</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>T</td>
<td>T</td>
<td>\bot</td>
</tr>
<tr>
<td>( \rho ) (Compr)</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>T</td>
</tr>
<tr>
<td>( \rho ) (NeedPub)</td>
<td>\bot</td>
<td>\bot</td>
<td>\bot</td>
<td>T</td>
<td>T</td>
<td>\bot</td>
</tr>
</tbody>
</table>
A Logical Framework for Evaluating Network Resilience Against Faults

A Incomplete Game Example

Outline:
- Introduction
- Model
- Strategy
- Conclusion

28/11/2007

2/11/2007

Exploit web server

Patch Email server

Exploit email server

Patch web server

Patch Email server
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 wins

Player can be taken by surprise
A Logical Framework for Evaluating Network Resilience Against Faults

The element of surprise

Outline:
- Introduction
- Model
- Strategy
- Conclusion

Exploit 4 in 3 unit → Network → Firewall 4 in 1 unit

28/11/2007

18
Anticipation games allows to model

- Denial of service
- Buffer overflow execution
- Permission abuse
- Cross-scripting
- Information leak
- ....
Rule Language

\[ F ::= A \quad \text{atomic propositions, in } A \]
\[ \top \quad \text{true} \]
\[ \neg F \quad \text{negation} \]
\[ F \land F \quad \text{conjunction} \]
\[ \Box F \]
\[ \Box_{\equiv} F \]
A successor node is compromised

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

\[ \text{Pre } Vu\text{ln} \land \text{Public} \land \neg \text{Compr} \]

\[ \text{Pre } Vu\text{ln} \land \text{Public} \land \neg \text{Compr} \]

\[ \text{Pre } \neg \text{Compr} \land \Diamond \text{Compr} \]

\[ \text{Pre } \text{Compr} \land \Diamond \neg \text{Compr} \]

\[ \text{Pre } \text{Public} \land \text{Vu}\text{ln} \]

\[ \text{Pre } \text{Public} \land \neg \text{Vu}\text{ln} \land \text{NeedPub} \]

\[ \text{Pre } \text{Vu}\text{ln} \land \neg \text{Compr} \]

\[ (2, I, \text{Compromise 0day}) \rightarrow \text{Compr} \]

\[ (7, I, \text{Compromise public}) \rightarrow \text{Compr} \]

\[ (4, I, \text{Compromise backward}) \rightarrow \text{Compr} \]

\[ (4, I, \text{Compromise forward}) \rightarrow \Diamond \text{Compr} \]

\[ (1, A, \text{Firewall}) \rightarrow \neg \text{Public} \]

\[ (1, A, \text{UnFirewall}) \rightarrow \text{Public} \]

\[ (3, A, \text{Patch}) \rightarrow \neg \text{Vu}\text{ln} \land \neg \text{Compr} \]
A Logical Framework for Evaluating Network Resilience Against Faults

A Play example

Outline:
- Introduction
- Model
- Strategy
- Conclusion

Player | Action | Rule | Target | Succ
--- | --- | --- | --- | ---
Admin | Execute | Patch Wall | 5 | 5
Intruder | Execute | Compromise Backward | 1 | 5

28/11/2007
Properties Semantic

\( \varphi ::= A \) atomic propositions, in \( A \)

\( \neg \varphi \)

\( \varphi \land \varphi \)

\( \Diamond \varphi \)

\( \Diamond \equiv \varphi \)

\( x + d_1 \leq y + d_2 \) clock constraints

\( x \cdot \varphi \) freeze

\( \{ P \} \Box \varphi \) invariant

\( \{ P \} \varphi_1 \cup \varphi_2 \) eventually

We abbreviate \( \{ P \} \text{TRUE} \cup \varphi \) as \( \{ P \} \Diamond \varphi \).
The player A have a strategy to satisfy the property $\varphi$

$\models \langle A \rangle \varphi$

In every future the node will be compromised

$\models \Box_{Compr}$
Properties Illustration

\[ \langle A \rangle \Box \Diamond \equiv \neg \text{Compr} \]

\[ \langle A \rangle \Box x \cdot \neg \Diamond \equiv \text{Avail} \Rightarrow \\
[ \langle A \rangle \Diamond y \cdot y \leq x + d \land \langle A \rangle \Box z \cdot z \leq y + d' \Rightarrow \\
\Diamond \equiv \text{Avail}] \]
Anticipation game are EXPTIME-complete
One More Thing!
Model and Strategies are fully implemented in C
The talk example cannot be analyzed by hand
4011 plays
40825 states
Future Work

Outline:
- Introduction
- Model
- Strategy
- Conclusion

Non determinism

Abstraction

CIA model
The framework

Outline:
- Introduction
- Model
- Strategy
- Conclusion
Analyzer Demo
Game and Time provide a richer model for intrusion analysis

Many directions to explore
During this work no network service was injured or tortured.
Rule execution time