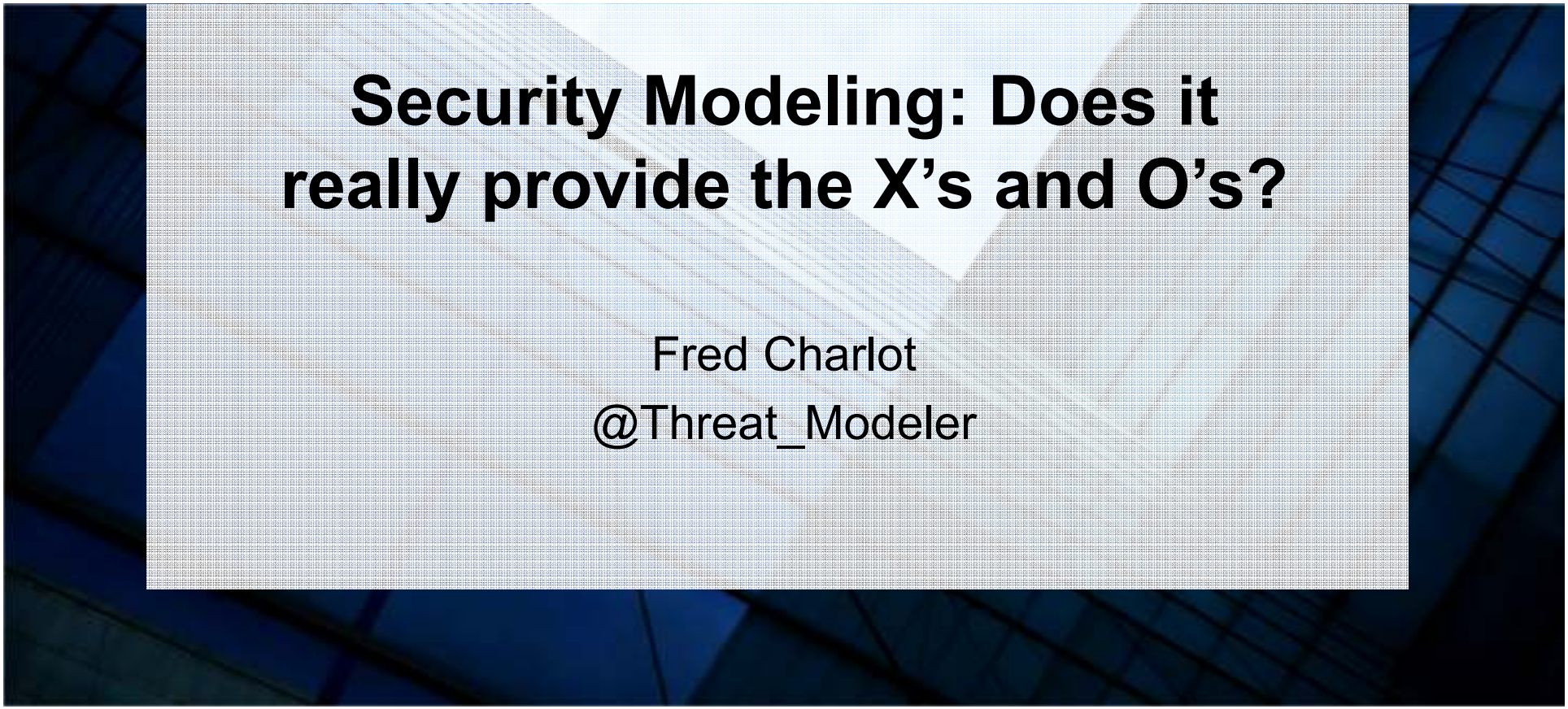
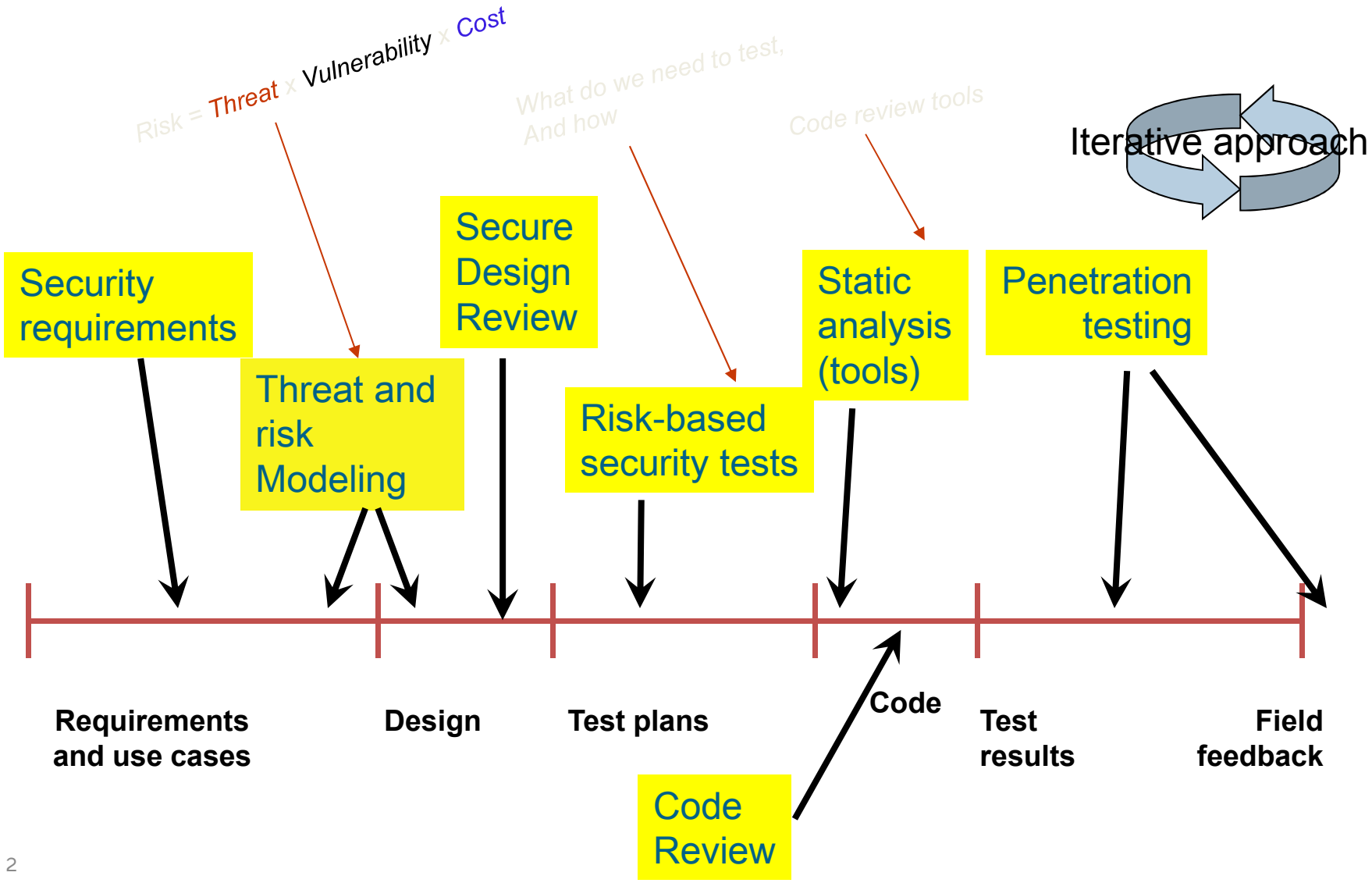

BERKELEY
RESEARCH
GROUP
Security Modeling: Does it really provide the X's and O's?
Fred Charlot
@Threat_Modeler

OWASP

BERKELEY RESEARCH GROUP



“Individual commitment to a group effort - that is what makes a team work, a company work, a society work, a civilization work. “

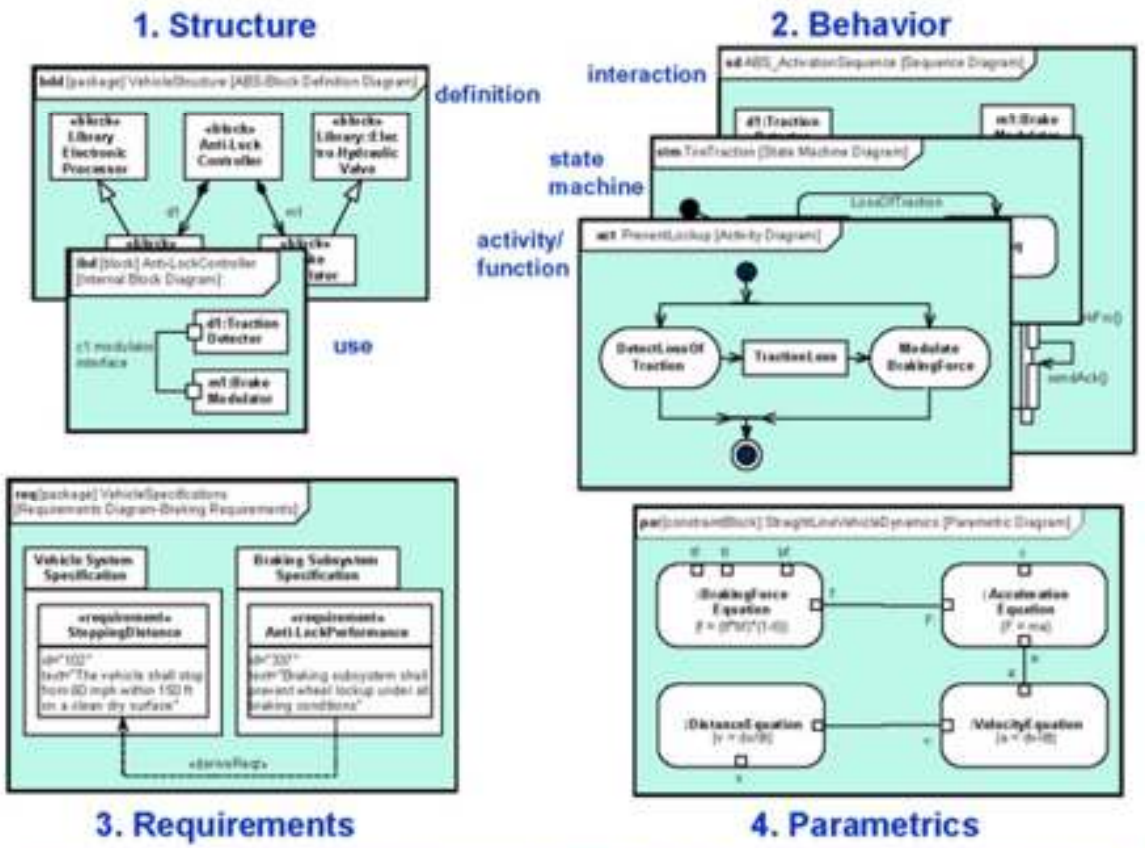
--Vince Lombardi

Software & System Modeling

BERKELEY RESEARCH GROUP

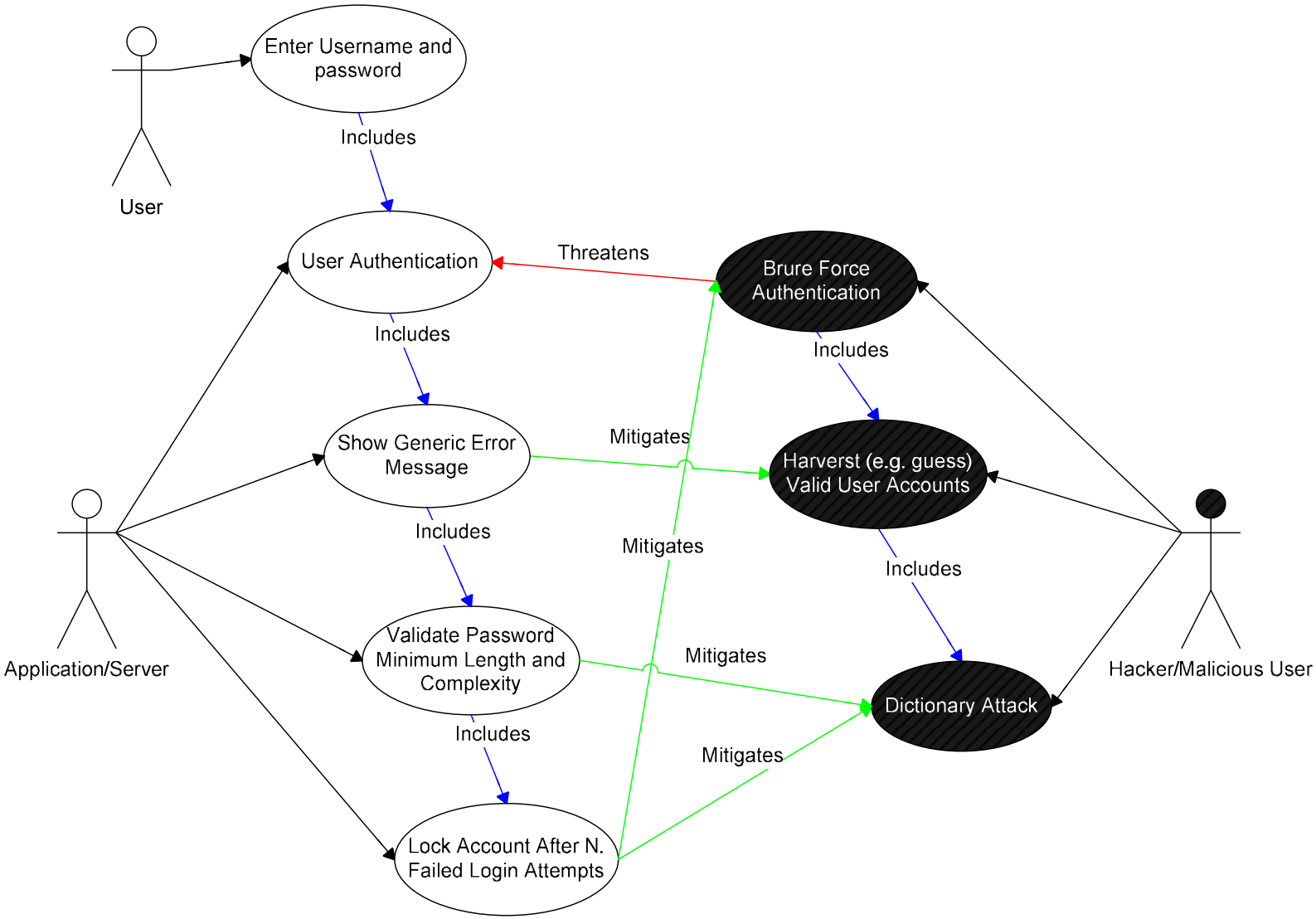
UNIFIED MODELING LANGUAGE™

OMG SYSTEMS MODELING LANGUAGE™



Note that the Package and Use Case diagrams are not shown in this example, but are respectively part of the structure and behavior pillars

Start with requirements

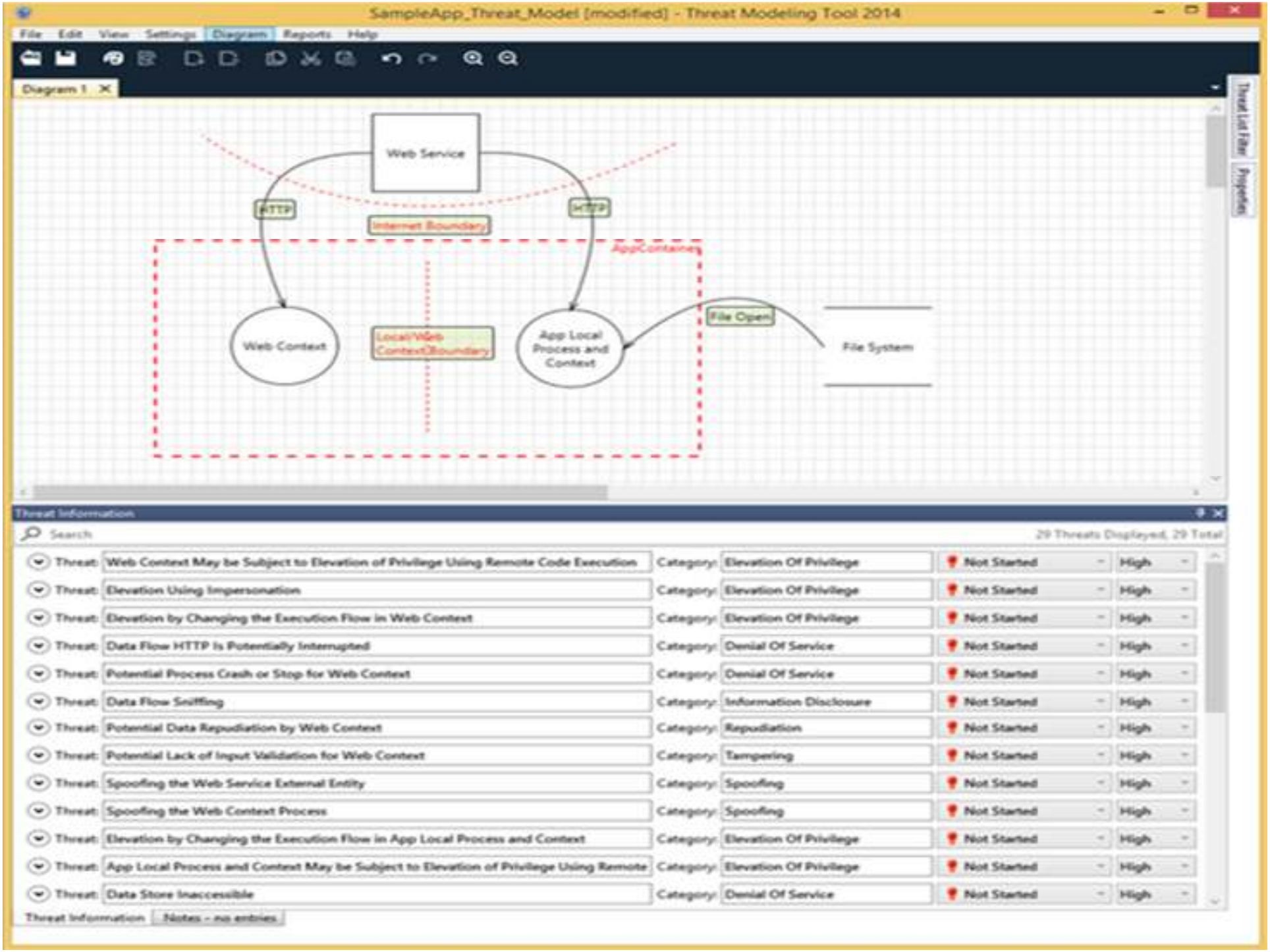


Types of diagrams

BERKELEY RESEARCH GROUP

Trust Boundary versus Attack Surface

- Block definition diagram (BDD)
- Internal block diagram (IBD)
- Use case diagram
- Activity diagram
- Sequence diagram
- State machine diagram
- Parametric diagram
- Package diagram
- Requirements diagram


SampleApp_Threat_Model [modified] - Threat Modeling Tool 2014
File Edit View Settings Diagram Reports Help
Diagram 1
Web Service
HTTP
HTTP
Internet Boundary
AppContainer
Web Context
Local/Web Context Boundary
App Local Process and Context
File Open
File System
Threat Information
Search
29 Threats Displayed, 29 Total
Threat: Web Context May be Subject to Elevation of Privilege Using Remote Code Execution Category: Elevation Of Privilege Not Started High
Threat: Elevation Using Impersonation Category: Elevation Of Privilege Not Started High
Threat: Elevation by Changing the Execution Flow in Web Context Category: Elevation Of Privilege Not Started High
Threat: Data Flow HTTP Is Potentially Interrupted Category: Denial Of Service Not Started High
Threat: Potential Process Crash or Stop for Web Context Category: Denial Of Service Not Started High
Threat: Data Flow Sniffing Category: Information Disclosure Not Started High
Threat: Potential Data Repudiation by Web Context Category: Repudiation Not Started High
Threat: Potential Lack of Input Validation for Web Context Category: Tampering Not Started High
Threat: Spoofing the Web Service External Entity Category: Spoofing Not Started High
Threat: Spoofing the Web Context Process Category: Spoofing Not Started High
Threat: Elevation by Changing the Execution Flow in App Local Process and Context Category: Elevation Of Privilege Not Started High
Threat: App Local Process and Context May be Subject to Elevation of Privilege Using Remote Category: Elevation Of Privilege Not Started High
Threat: Data Store Inaccessible Category: Denial Of Service Not Started High
Threat Information
Notes - no entries

"You just have to watch film, study your opponent, make yourself better all week…"

-- Head Football Coach Kevin Sumlin

Kill Chain

BERKELEY RESEARCH GROUP

Lockheed Martin's Cyber Kill Chain

Threat Enumeration

BERKELEY RESEARCH GROUP

STRIDE-per-element,

STRIDE-per-interaction

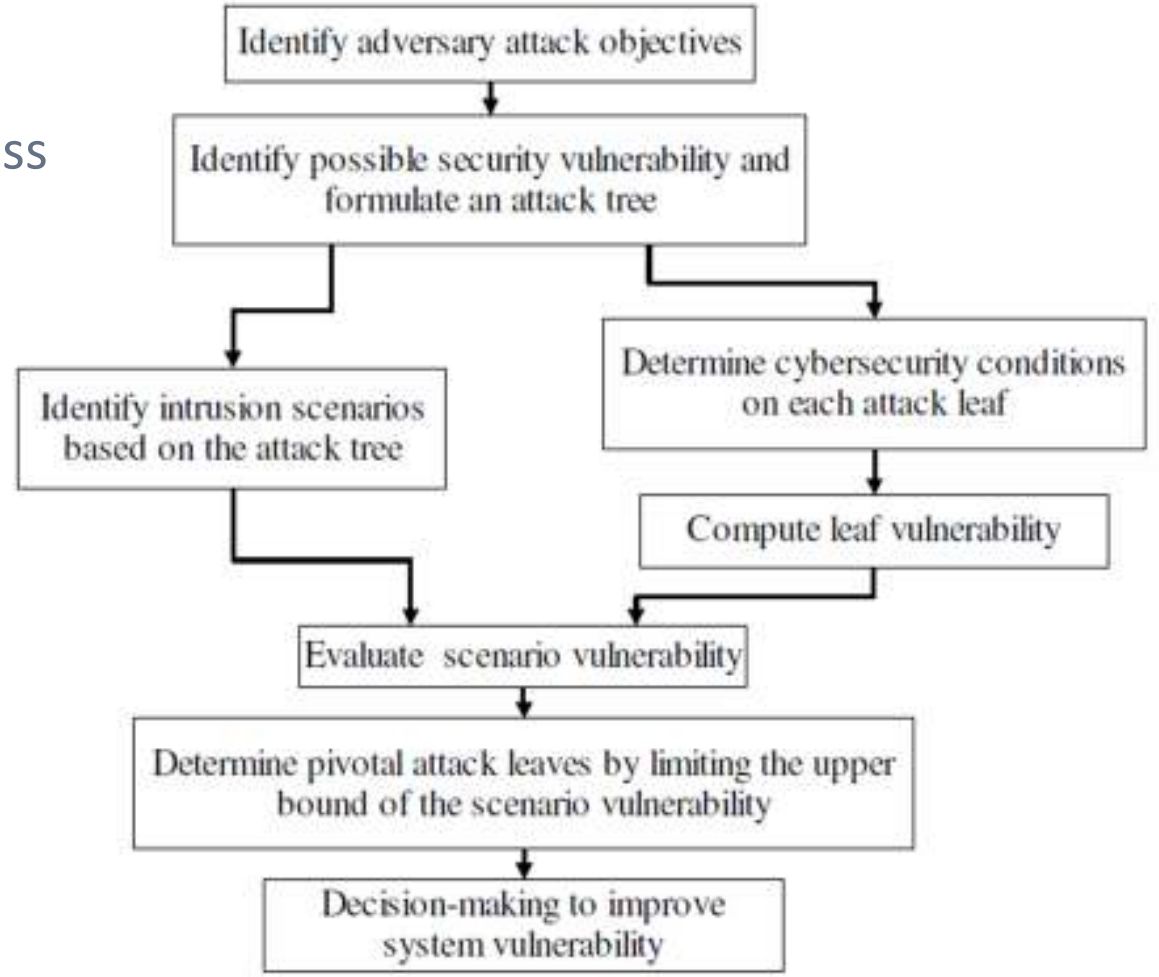
- Spoofing
- Tampering,
- Repudiation,
- Information Disclosure,
- Denial of Service,
- Elevation of Privilege

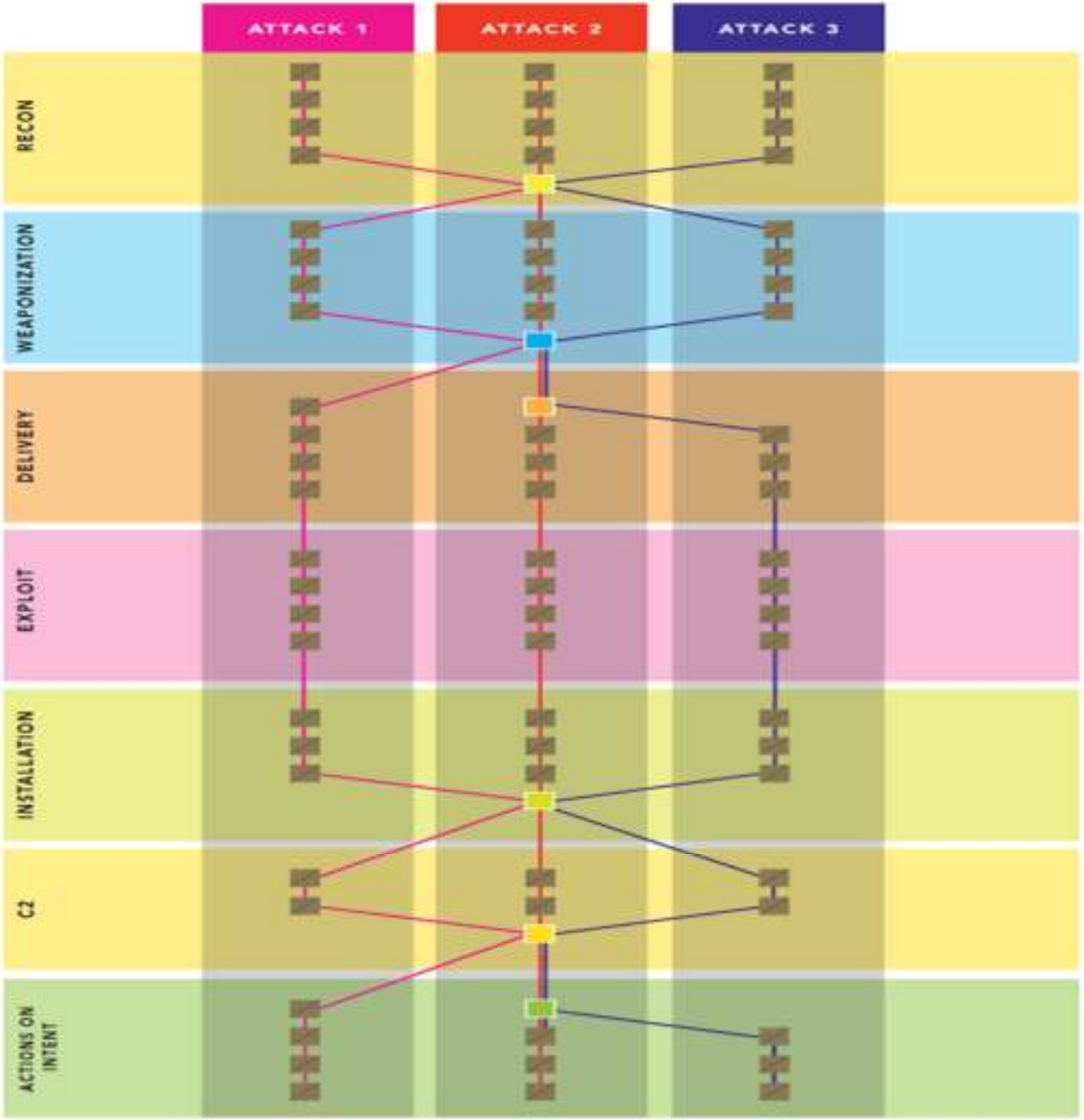
	S	T	R	I	D	E
External Entity	x		x			
Process	x	x	x	x	x	x
Data Flow		x		x	x	
Data Store		x	?	x	x	

- **Start with external entities**
- **Never ignore a threat because it's not what you're looking for**
- **Focus on feasible threats**

Attack Trees

1. Create a root
2. Create subnodes
3. Consider completeness
4. Prune the tree.





BERKELEY RESEARCH GROUP

Attack Libraries

BERKELEY RESEARCH GROUP

- Metasploit
  - http://www.rapid7.com
- CAPEC
  - https://capec.mitre.org/
- OWASP
  - https://www.owasp.org/index.php/Attacks

Now it’s time to become what we are, which is a gameplan defense, meaning every week we come in and we look at what the opponent does and try to gameplan the opponent.

-- Unknown

Impact/Likelihood

BERKELEY RESEARCH GROUP

FAIR's risk decomposition

1. Identify Components
2. Evaluate frequency
3. Estimate probability
4. Derive Risk

DREAD risk decomposition

1. Damage - how bad would an attack be?
2. Reproducibility - how easy is it to reproduce the attack?
3. Exploitability - how much work is it to launch the attack?
4. Affected users - how many people will be impacted?
5. Discoverability - how easy is it to discover the threat?

RISK

BERKELEY RESEARCH GROUP

Step 1 - System Characterization

Step 2 - Threat Identification

Step 3 - Vulnerability Identification

Step 4 - Control Analysis

Step 5 - Likelihood Determination

Step 6 - Impact Analysis

Step 7 - Risk Determination

Step 8 - Control Recommendations

Use Case

BERKELEY RESEARCH GROUP

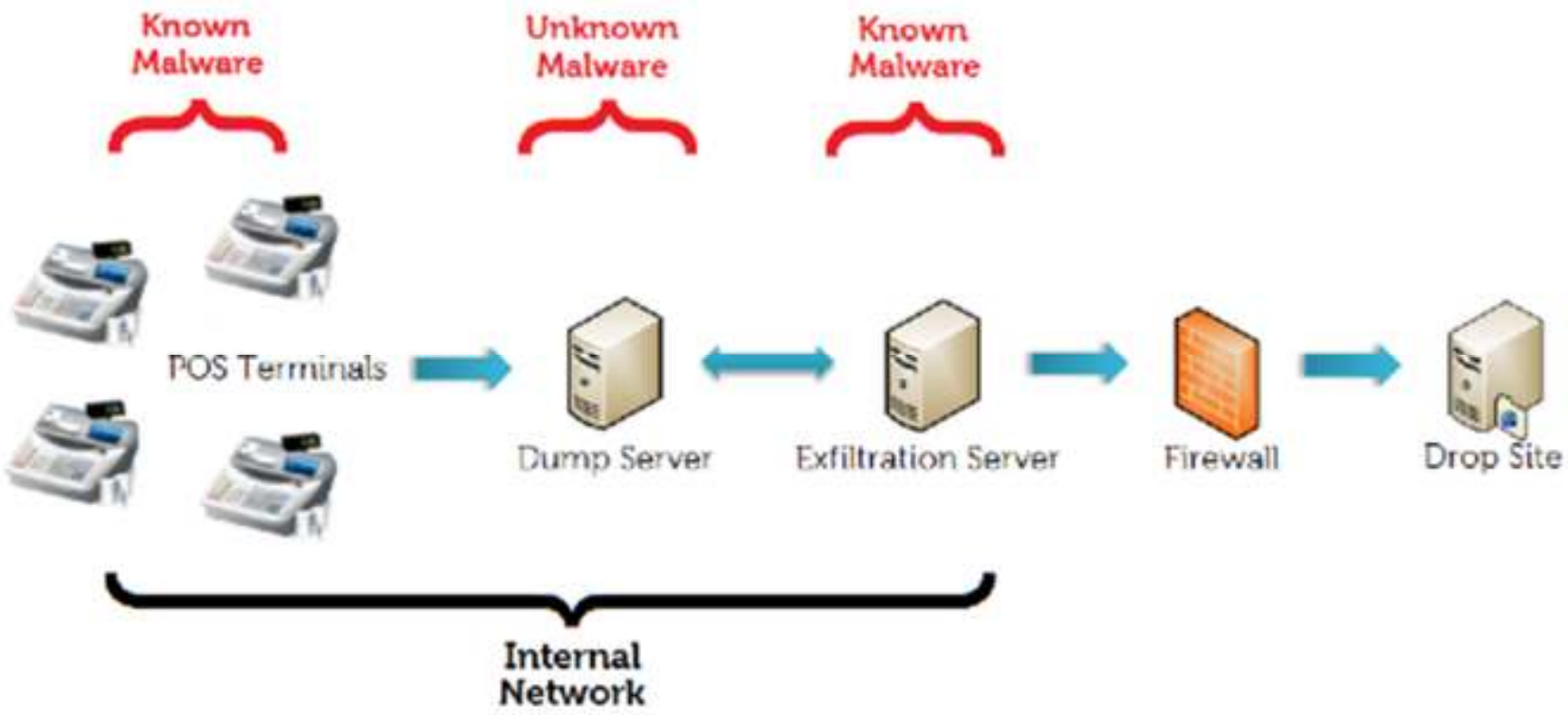
Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Reconnaissance	Threat Intelligence NIDS D/B Security	Information Sharing Policy				
Weaponization	Threat Intelligence NIDS					
Delivery	Context-Aware Endpoint Malware Protection	Change Management File Integrity Application Whitelisting NIPS	Inline AV	Queuing		Router ACLs App-Aware Firewall Trust Zones Inter-Zone NIPS
Exploitation	Endpoint Malware Protection	Secure Password	DEP			App-Aware Firewall Trust Zones Inter-Zone NIPS
Persistence / Lateral Movement	Log Monitoring	Privilege Separation Secure Password Two- Factor	Router ACLs AV			App-Aware Firewall Trust Zones Inter-Zone NIPS
Command & Control	NIDS	Firewall ACL	NIPS	Tarpit	DNS Redirect	Trust Zones DNS Sinkholes
Actions on Targets	Endpoint Malware Protection	Encryption	Endpoint Malware Protection	Quality of Service	Honeypot	Incident Response
Exfiltration	DLP	Egress Filtering	DLP			Firewall ACLs

BERKELEY RESEARCH GROUP

Kill Chain Analysis of Target Data Breach

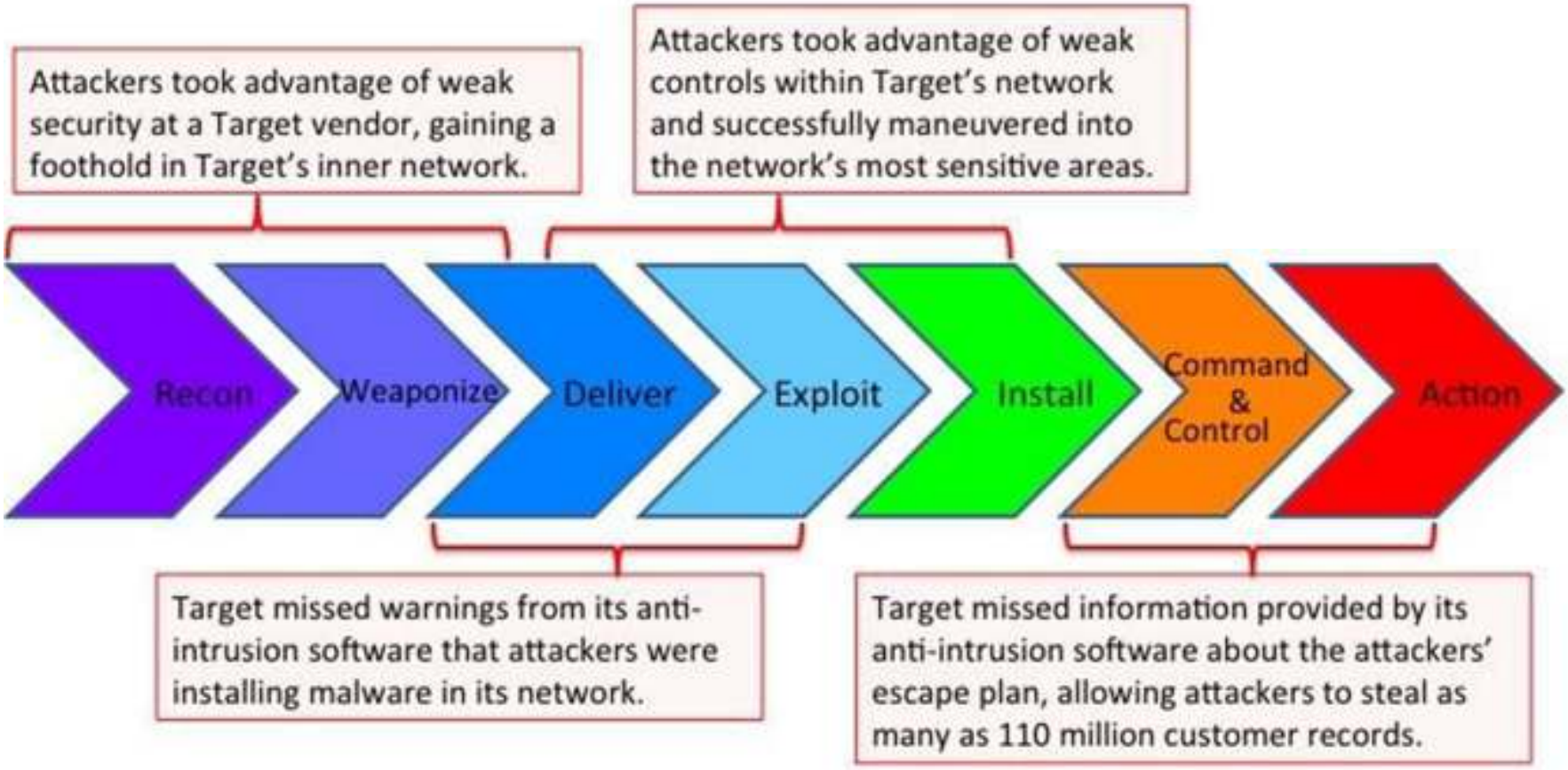
From

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

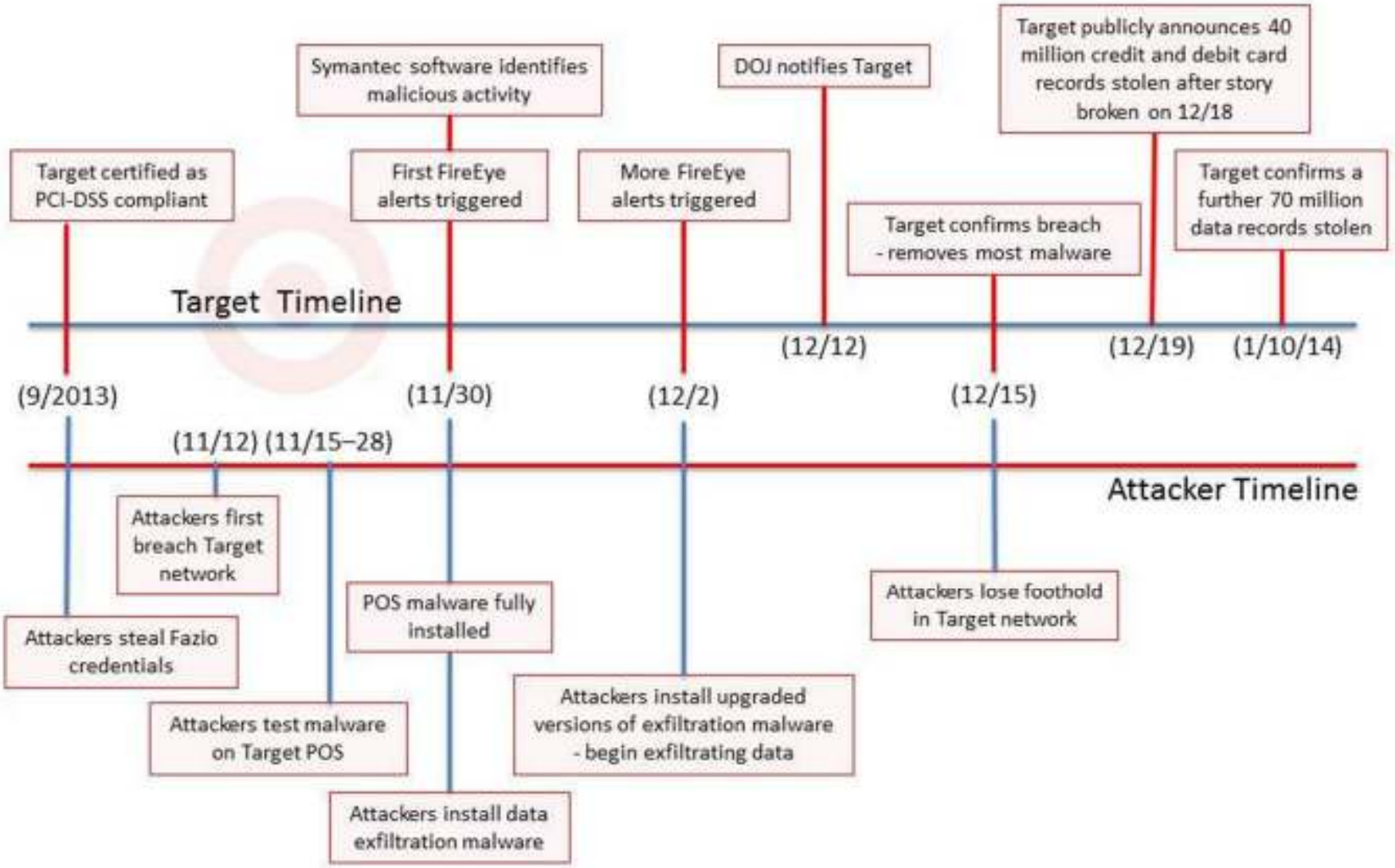

Known Malware
Unknown Malware
Known Malware
POS Terminals
Dump Server
Exfiltration Server
Firewall
Drop Site
Internal Network

Missed Opportunities

BERKELEY RESEARCH GROUP



Timeline


Target certified as PCI-DSS compliant
Symantec software identifies malicious activity
First FireEye alerts triggered
More FireEye alerts triggered
DOJ notifies Target
Target confirms breach - removes most malware
Target publicly announces 40 million credit and debit card records stolen after story broken on 12/18
Target confirms a further 70 million data records stolen
Target Timeline
(9/2013)
(11/30)
(12/2)
(12/12)
(12/15)
(12/19)
(1/10/14)
(11/12) (11/15–28)
Attacker Timeline
Attackers first breach Target network
Attackers steal Fazio credentials
Attackers test malware on Target POS
POS malware fully installed
Attackers install data exfiltration malware
Attackers install upgraded versions of exfiltration malware - begin exfiltrating data
Attackers lose foothold in Target network

Thank You!

Fred Charlot| Principal

Berkeley Research Group, LLC

700 Louisiana Street, Ste. 2600 | Houston, TX 77002

D 713.493.9410 | O 713.481.9410 |

M 713.412.4105 | F 713.236.8596

@Threat_Modeler

fcharlot@brg-expert.com | www.brg-expert.com

References

- http://docs.ismgcorp.com/files/external/Target_Kill_Chain_Analysis_FINAL.pdf
- http://www.microsoft.com/en-us/download/details.aspx?id=42518
- https://www.owasp.org/index.php/OWASP_Threat_Modelling_Project
- **Threat Modeling: Designing for Security, By:** Adam Shostack