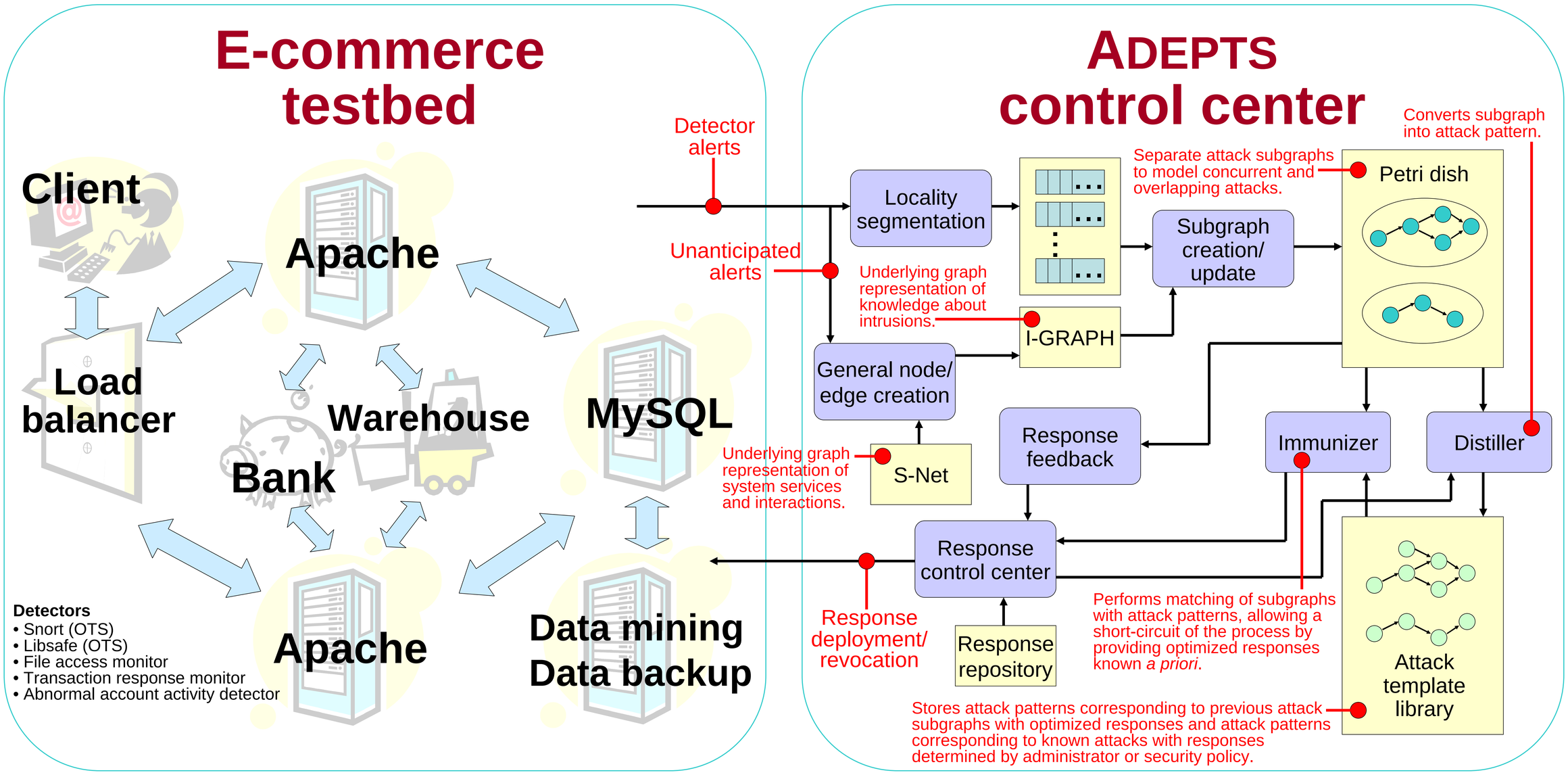
CERIAS

ADEPTS: Automated Adaptive Intrusion Response

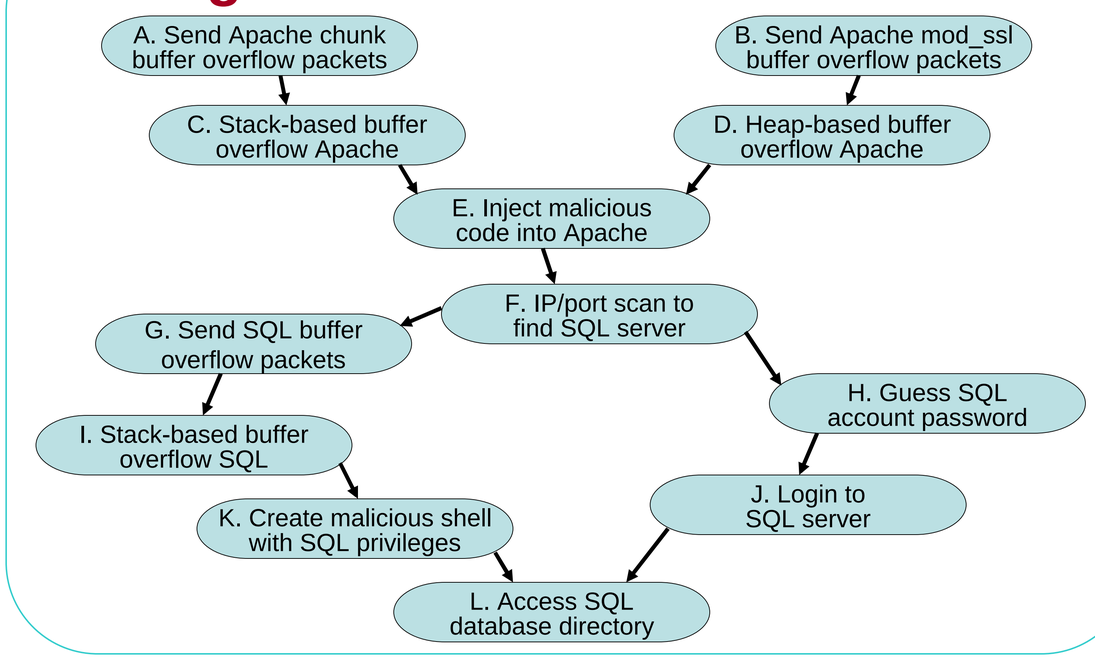
Yu-Sung Wu Bingrui Foo Matthew Glause Saurabh Bagchi Eugene Spafford

Goal: To design an automated intrusion response system that increases the survivability of distributed systems

Key features
- Adaptation in response decision algorithm
- Attack pattern matching for known attacks
- Ability to handle unanticipated attacks



Fragment of an attack scenario



Attack instance	(Responses deployed), after which step, (S|F)	Steps achieved before attack stopped
1	(R0,R1), C, (F) (R2,R3), F, (S)	A, C, E, F
2	(R4), F, (F) (R5,R6), L, (S)	B, D, E, F, H, J, L
3	(R7,R8), C, (S)	A, C
4	(R9), F, (S)	B, D, E, F

Response	Description
R0	Block attacker IP from port 80 of Apache server
R1	Make Apache image read-only
R2, R5, R8, R9	Block attacker IP from accessing Apache server
R3, R7	Restarting Apache server
R4	Block attacker IP from port 443 of Apache server
R6	Restart MySQL server

Current work
- Synthesize new responses at runtime
- Variable expiration periods of responses
- Optimality of responses