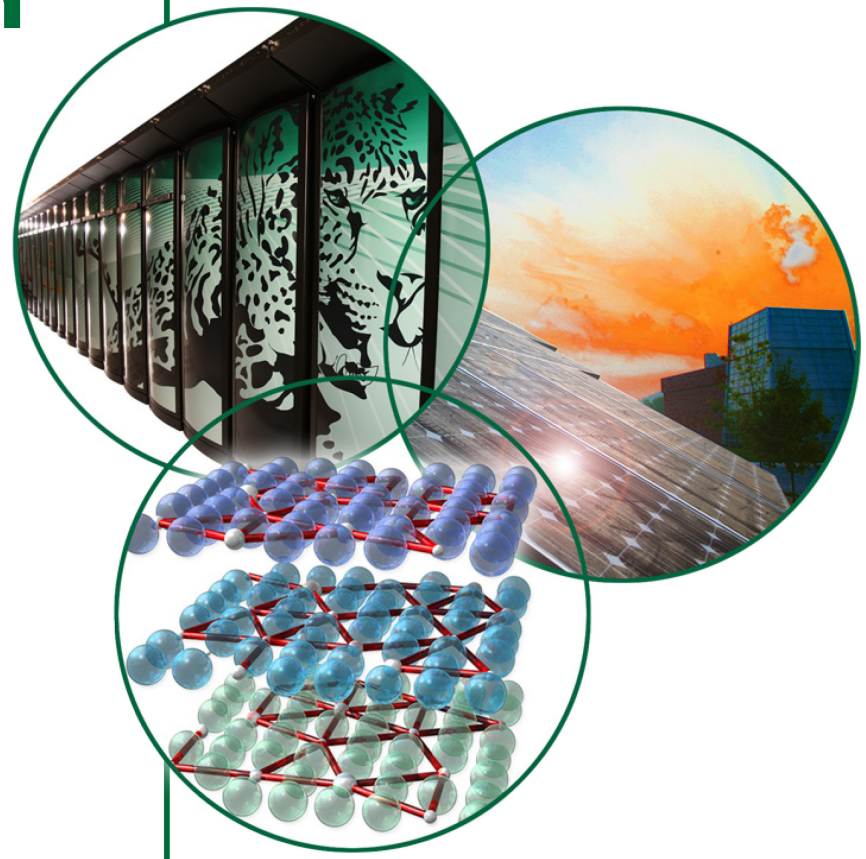
Information Security Analysis Using Game Theory and Simulation

Presented at:
WORLDCOMP'12
SAM'12 / STMACIP'12

Las Vegas, NV

Robert K. Abercrombie, Ph.D.

July 18, 2012



Authors:
Bob G. Schlicher and
Robert K. Abercrombie

U.S. DEPARTMENT OF ENERGY

The submitted manuscript has been authored by a contractor of the U.S. Government under contract DE-AC05-00OR22725. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

OAK RIDGE NATIONAL LABORATORY
MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

Agenda For Today's Presentation

- Purpose
  - Present current findings of our investigation of Information Security Analysis using Game Theory and Simulation
- Introduction
- Game and Simulation Basis
- Game Scenarios
- Setting up the Game (Allowable States, Actions and Parameter Sets)
- Graphical Results of the Simulation
  - Probability of successful attacks in the enterprise network
  - Confidentiality dynamics of $P_{workstation_data_stolen}$ in the enterprise network
  - Integrity of dynamics of $P_{Website_defaced}$ in the enterprise network
  - Availability dynamics of $P_{Webserver_DOS}$ in the enterprise network
- Conclusions and Future Directions

Introduction –
Definitions of Confidentiality, Integrity, and Availability

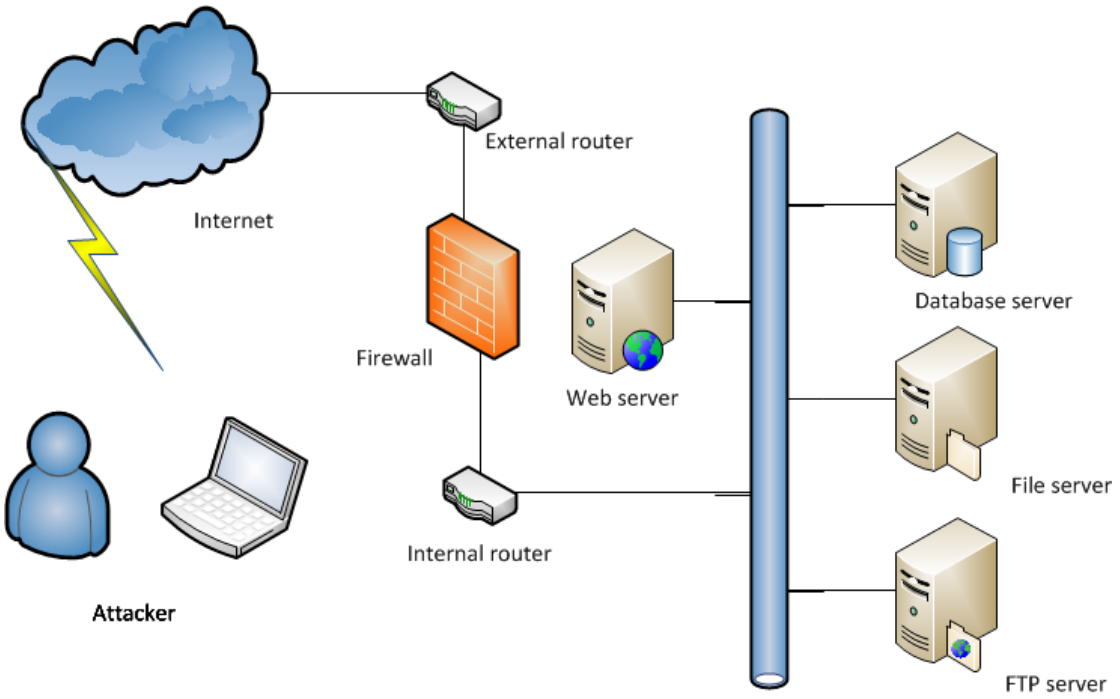
- **44 U.S. Code 3502**
  - **defines Information Security as a means of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:**
    - ***confidentiality***, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
    - ***integrity***, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; and
    - ***availability***, which means ensuring timely and reliable access to and use of information

Introduction –
Information Security Analysis Using Game Theory and Simulation

- Information security analysis can be performed using game theory implemented in dynamic simulations of Agent-Based Models (ABMs).
  - Such simulations can be verified with the results from game theory analysis, and
  - further used to explore larger scale, real world scenarios involving multiple attackers, defenders, and information assets.
- Current models only consider perfect information assuming that the defender is always able to detect attacks;
  - Assuming that the state transition probabilities are fixed before the game,
  - assuming that the players' actions are always synchronous, and
  - that most models are not scalable with the size and complexity of systems under consideration.
- Our approach addresses:
  - Imperfect information and scalability that allows us to also address previous limitations of current stochastic game models.
  - Our use of ABMs yields results of selected experiments that demonstrate our approach and provides a quantitative measure for realistic information systems and the related security scenarios.

Game and Simulation Basis

- Architecture
  - Internet
  - External router
  - Firewall
  - Internal router
  - Servers
    - Web server
    - Database server
    - Filer Server
    - FTP Server



- Players – Attacker and Defender (System Administrator)

Game and Simulation Basis (cont.)

- ABMs bring significant benefits when:
  - (1) interactions between the agents are complex, nonlinear, discontinuous or discrete;
  - (2) space is crucial and the agents' positions are not fixed;
  - (3) the population is heterogeneous;
  - (4) the topology of the interactions are heterogeneous and complex; or
  - (5) the agents exhibit complex behavior, including learning and adaptation.

Game and Simulation Basis (cont.)

- The administrator performs:
  - actions that begin with the probability of detecting something wrong.
- Since the enterprise state is known, the simulation limits the administrator's actions,
  - which for the most part is a possible counter action to the most current action performed by the attacker.
  - A reasonable assumption in that a competent administrator is assumed to be able to recognize a problem with their system.
- Before the administrator performs any counter action,
  - a detection action is required to confirm the type of attack.
  - In the simulation, our time unit represents one minute.
- We executed 1,000 simulations with each simulation spanning 250 simulated minutes.
  - Experimental results were aggregated into bins (10 minute intervals) and averaged to arrive at the probabilities of attack success.

Game Scenarios – Scenario 1 of 4

- Scenario 1 – httpd hacked and recovered
  - Hypertext Transfer Protocol Daemon (i.e. web server) is hacked by an attacker and is successfully recovered by the administrator
  - Probability of Action P(a), Probability of Success P(s), Payoff (+/- minutes)

Scenario 001. httpd is hacked and recovered	Simulation parameters and notes
1. The attacker attacks an httpd process.	Attack_http, P(a)=0.5, P(s)=1.0
2. The attacker continues the attack to compromise the httpd.	continue_attacking, P(a)=0.5, P(s)=0.5
3. The attacker compromises the httpd system, httpd has been hacked.	State change to Httpd_hacked.
4. The admin detects the hacked httpd.	detect_httpd_hacked, P(a)=0.5, P(s)=0.5, payoff = -1.
5. The admin removes the compromised account and restarts httpd.	remove_compromised_account_restart_ httpd, P(a)=1.0, P(s)=1.0, payoff= -20.

Game Scenarios – Scenarios 2, 3, 4 of 4

- Scenario 2 – Deface Web Site with System Administrator Correction
- Scenario 3 – Denial of Service (DOS) with System Administrator Correction
- Scenario 4 – File Server Data Stolen with System Administrator Correction

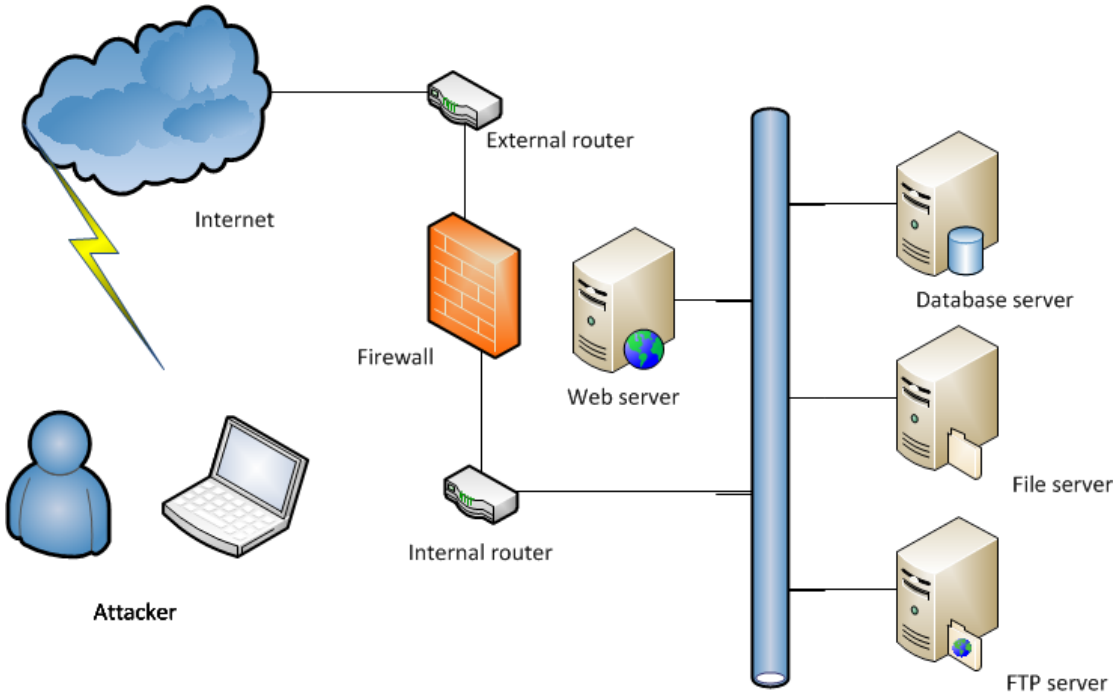
Scenario 002. Deface Web Site
1. The httpd is hacked, but not recovered (see Scenario 001).
2. The attacker defaces the web site.
3. The admin detects the defaced web site.
4. The admin restores the website and removes the compromised account.

Scenario 003. Denial of Service (DOS)
1. The httpd is hacked, but not recovered (see Scenario 001).
2. The attacker installs a sniffer and a backdoor program.
3. The attacker runs a DOS virus on the web server.
4. The network traffic load increases and degrades the system.
5. The admin detects the traffic volume and identifies a DOS attack.
6. The admin removes the DOS virus and the compromised account.

Scenario 004. File Server Data Stolen
1. The httpd is hacked, but not recovered (see Scenario 001).
2. The attacker installs a sniffer and a backdoor program.
3. The attacker attempts to crack the file server root password.
4. The attacker cracks the password; the file server is hacked.
5. The attacker downloads data from file server.
6. The admin detects the file server hack.
7. The admin removes the file server from the network.

Setting up the Game (Allowable States)

1. normal_operation
2. httpd_attacked
3. httpd_hacked
    a. detect. hacked_detected
4. ftpd_attacked
5. ftpd_hacked
6. website_defaced
    a. detect. website_defaced_detected
7. webserver_sniffer
8. webserver_sniffer_detector
9. webserver_dos_1
    a. detect. webserver_dos_1_detected
10. webserver_dos_2
11. fileserver_hacked
    a. detect. fileserver_hacked_detected
12. fileserver_data_stolen_1
13. workstation_hacked
    a. detect. workstation_hacked_detected
14. workstation_data_stolen_1
15. network_shut_down



Setting up the Game (Allowable for Players)

Attacker's Actions	Defender's Actions
• Attack_httpd	• Remove_compromised_account_-restart_httpd
• Attack_ftpd	• Restore_Website_remove_-compromised_account
• Continue_attacking	• Remove_virus_and_compromised_-account
• Deface_website_leave	• Install_sniffer_detector
• Install_sniffer	• Remove_sniffer_detector
• Run_DOS_virus	• Remove_compromised_account_-restart_ftpd
• Crack_file_server_root_password	• Remove_compromised_account_-sniffer
• Crack_workstation_root_password	
• Capture_data	
• Shutdown_Network	

Setting up the Game –
Parameter Modeling Set – Attacker

- Probability of Action, Probability of Success, Payoff (minutes), Resulting Allowable transitions from state to state

Action Name	Prob. Action	Prob. Success	Payoff	State From	State To
Attack_httpd	0.5	0.5	10	1	2
Continue_attacking	0.5	0.5	0	2	3
Deface_website_leave	0.5	0.5	99	3	6
Install_sniffer	0.5	0.5	10	3	7
Run_dos_virus	0.5	0.5	30	7	9
Crack_file_server-root-pw	0.5	0.5	50	7	11
Capture_data_file_-server	0.5	0.5	999	11	12
Shutdown_network	0.5	0.5	999	9	15

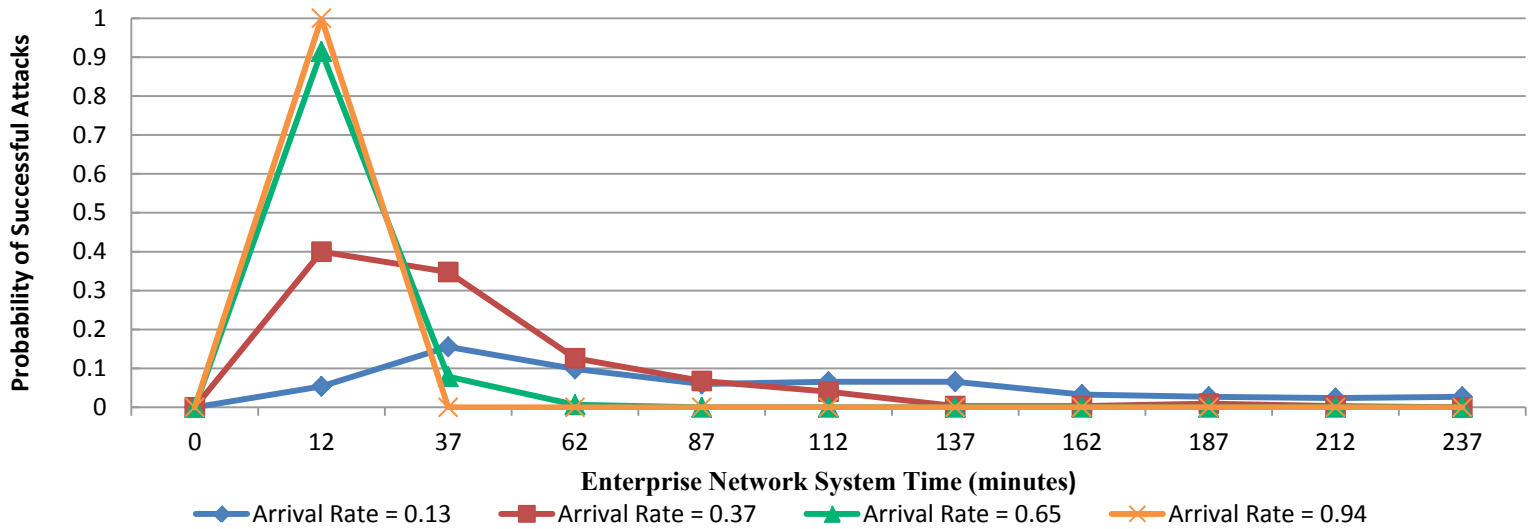
Setting up the Game –
Parameter Modeling Set - Defender (Administrator)

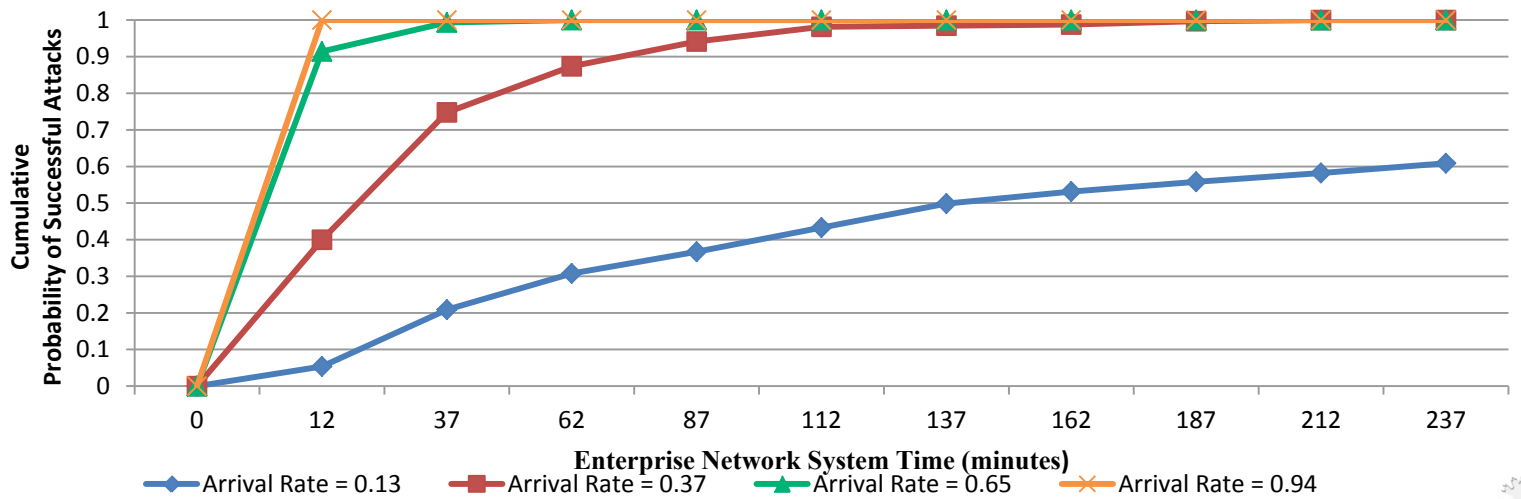
- **Probability of Action/Success, Payoff (+/- minutes), States (from/to)**

Action Name	Prob. Action	Prob. Success	Payoff	State From	State To
Detect_httpd_hacked	0.5	0.5	1	3	3a
Detect_defaced_website	0.5	0.5	-1	6	6a
Detect_webserver_sniffer	0.5	0.5	-1	7	8
Remove_sniffer	1.0	1.0	0	8	1
Remove_compromised_-account_restart_httpd	1.0	1.0	10	3a	1
Restore_website_remove_-compromised_account	1.0	1.0	-10	6a	1
Detect_dos-virus	0.5	0.5	-1	9	9a
Remove_virus-and_-compromised_account	1.0	1.0	-3.0	9a	1
Detect_fileserver_hacked	0.5	0.5	-1	11	11a
Detect_fileserver_hacked	0.5	1.0	-1	11	11a
Remove_compromised_-account_restore_fileserver	1.0	1.0	-20	11a	1

Probability of Successful Attacks in the Enterprise Network (Attacks ~ every 1, 1.5, 2.7, & 7.7 minutes)

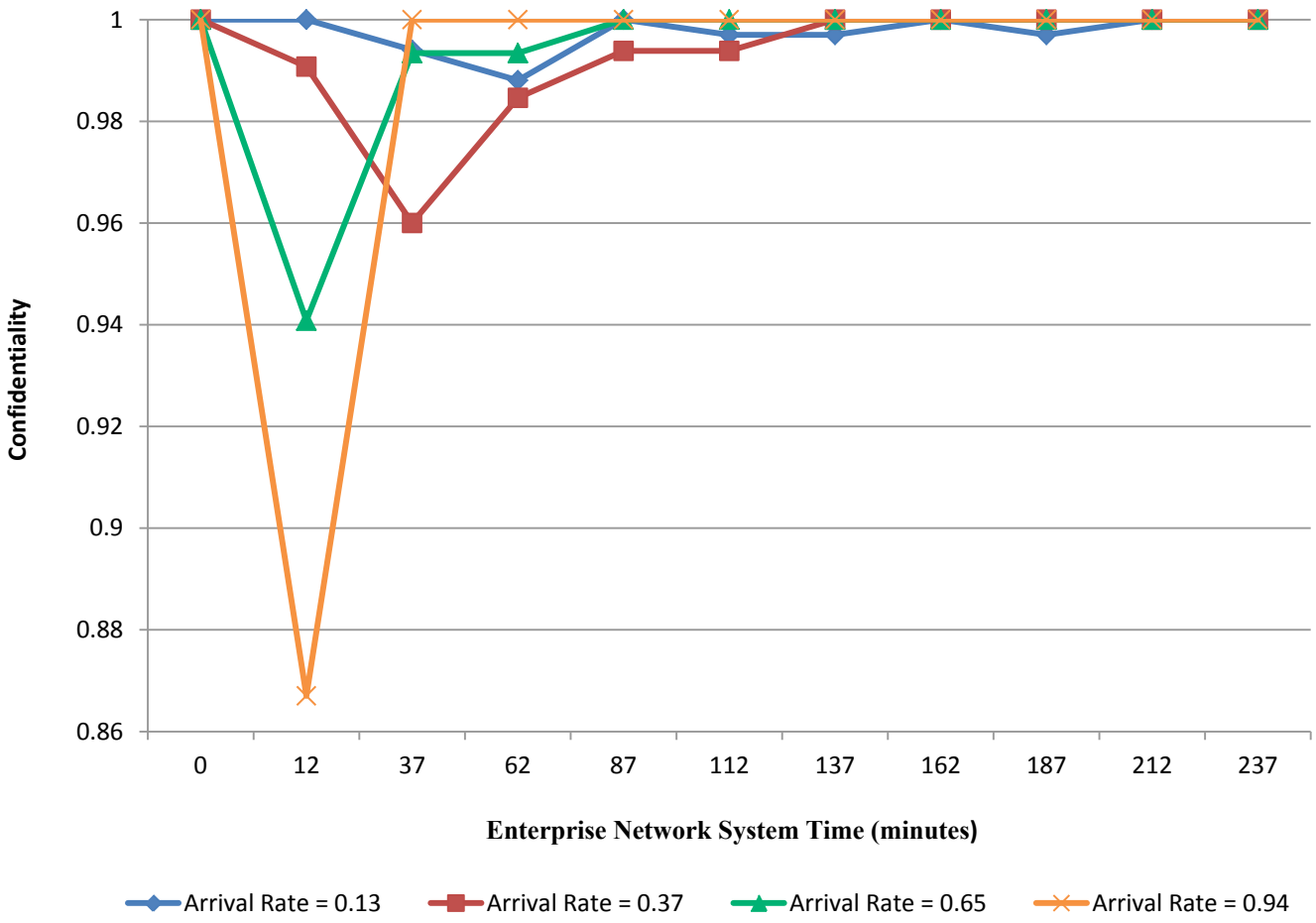
- Attacker has distinct advantage as arrival rates increase.





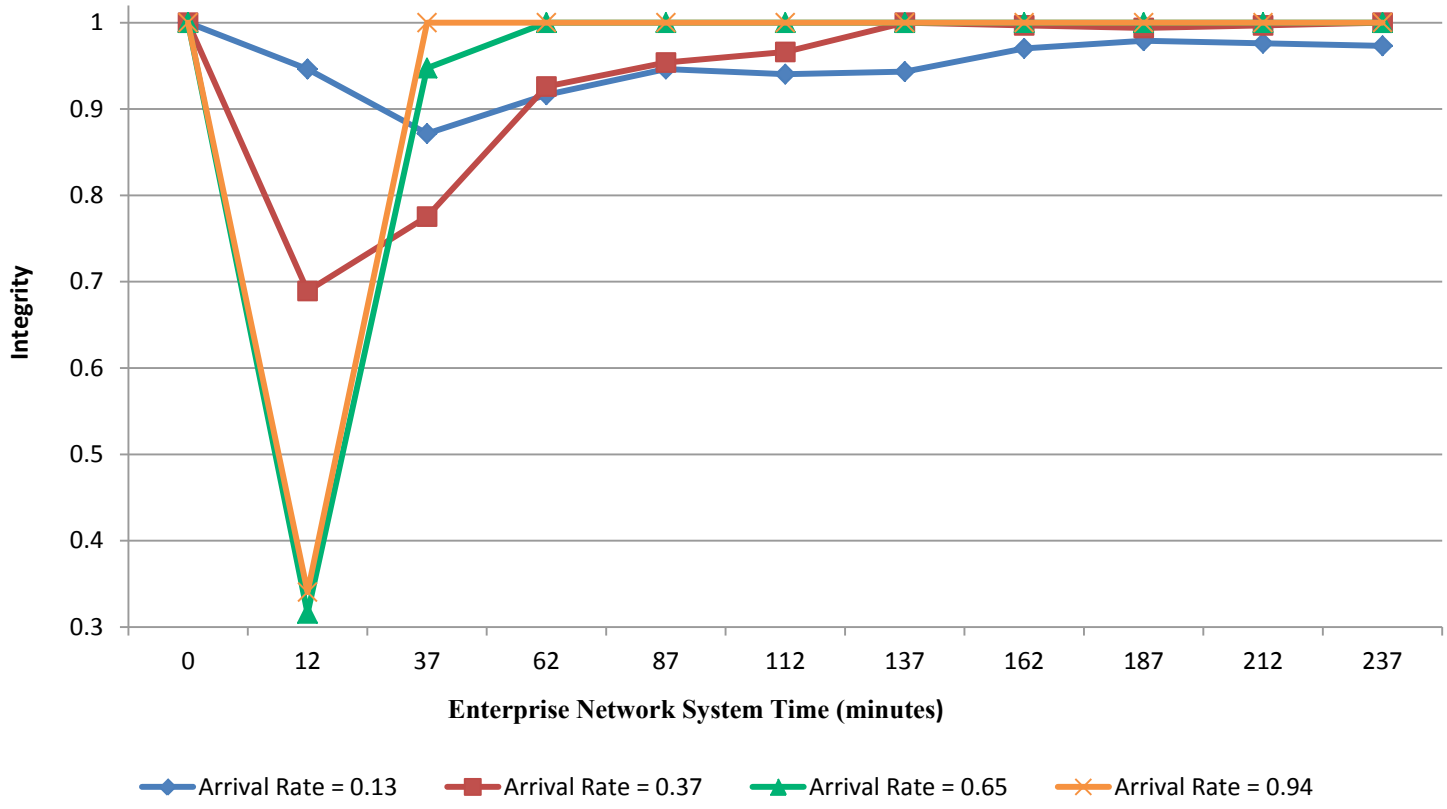
Confidentiality dynamics of $P_{workstation_data_stolen}$ in the enterprise network

- Confidentiality degrades then recovers over time.



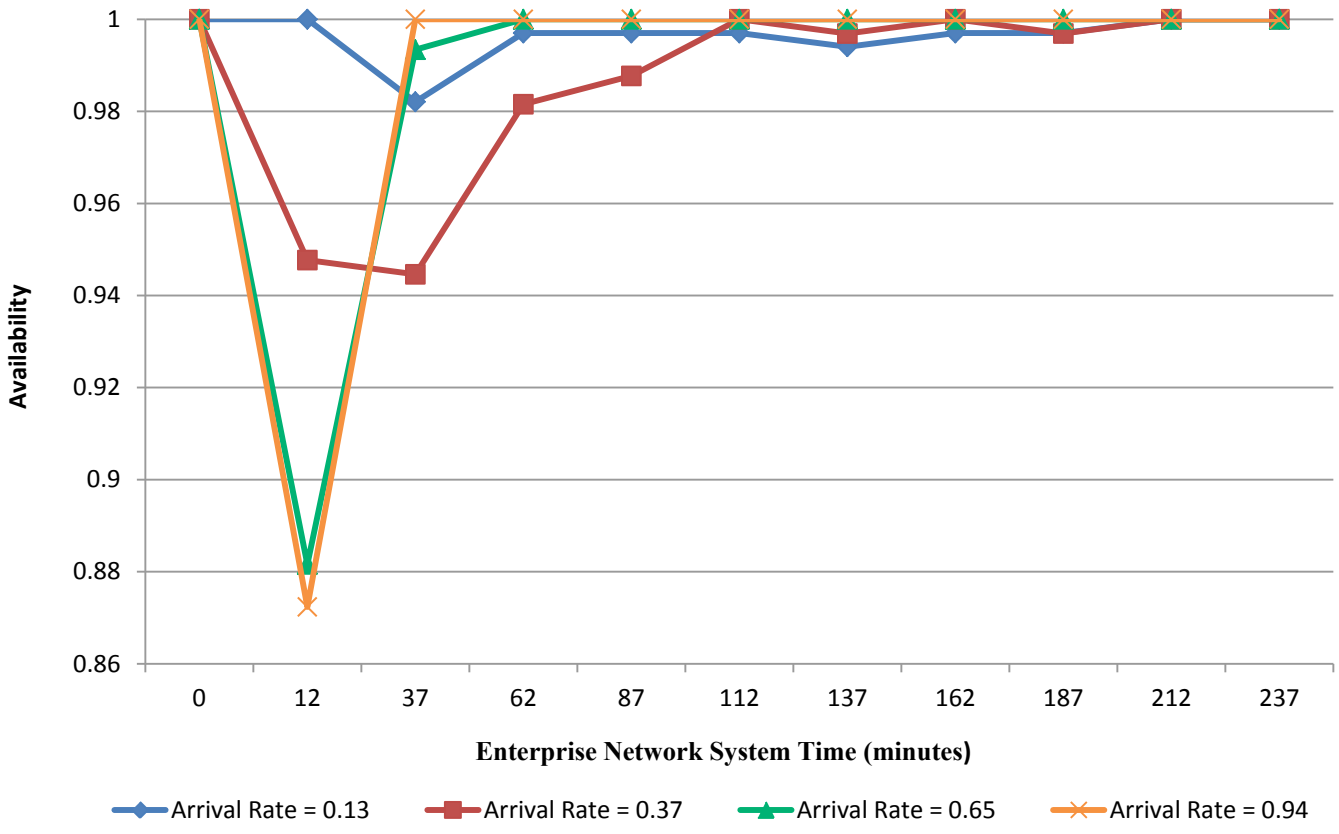
Integrity of dynamics of $P_{Website_defaced}$ in the enterprise network

- Integrity degrades then recovers over time.



Availability dynamics of $P_{Webserver_DOS}$ in the enterprise network

- Availability degrades then recovers over time.



Comparing Confidentiality, Integrity and Availability

- Confidentiality, Integrity and Availability of the Enterprise System:
  - Decreases at the beginning of the attack,
  - then increases over time,
  - as the administrator's action enable the enterprise to recover from the attack.
- Therefore, it is crucial to the safety of the enterprise system that
  - The administrator can discover the attack as early as possible.

Conclusions

- Our model is a simulation based on Agent Based Model (ABM) where the active components of the model, the agents, engage in interactions on scenario-by-scenario basis.
  - This is in contrast to the previous techniques that utilized nonlinear programming in MATLAB and Petri nets.
- The agents in the simulation include the Attacker and the Defender (i.e., administrator).
- The agents perform actions that can change the system state of the enterprise. For each state, agents are limited in the actions they can perform.
- Depending on the scenario, the attacker executes one of many actions with an associated probability of deciding to do the action and a probability that the action will be successful once the decision has been committed.
- Within each time unit (minute), the simulator thread visits each agent giving them the opportunity to perform an action or not.
  - We executed 1,000 simulations with each simulation spanning 250 simulated minutes.
  - Experimental results were aggregated into bins and averaged to arrive at the probabilities of attack success.

Future Directions

- One interesting finding we discovered during the analysis of the results, damage can occur in other states, while the initial attack is being repaired – a future endeavor.
- We also plan to broaden the field of play,
  - allowing multiple attacks from multiple agents to occur over the enterprise.
- An interesting theme will be to address unknown or zero-day attacks.
- We believe:
  - The ABM approach will provide security analysts with a useful decision-making tool for information security.
  - This tool will also provide security analysts and financial analysts a useful decision-making tool to augment analysis and investments decision making in the enterprise.

Oak Ridge National Laboratory:
Meeting the challenges of the 21st century

Robert K. Abercrombie, Ph.D., Bob G. Schlicher
Email: abercrombier@ornl.gov, schlicherbg@ornl.gov
Phone: (865) 241-6537, (865) 574-4988
http://www.ornl.gov/~abe