What Incidents Data Tell Us About Attackers: 
Analysis of Incident Reports from a Shared Computing Infrastructure

Jianxiong Gao, University of Illinois at Urbana-Champaign

ADVISORS: Prof. Zbigniew T. Kalbarczyk, Rafael Bonilla

Background

- Analysis based on 130 incident reports from NCSA since 2007.
- Initially, incidents classified as:
  i. Detected
  ii. Missed
  iii. False positive

- Seven phases of an attack:
  1. Scan
  2. Breach
  3. Penetration
  4. Control
  5. Embedding
  6. Data Modification
  7. Attack-relay/misuse

- Three main types of alerts:
  1. IDS (intrusion detection system): a protocol-based detection tool
  2. NetFlow analyzers: monitor the network
  3. External notifications: external users or third-party partners

Key observations:

- About 20% of the incidents are missed
- About 21% of the incidents are false positives

Lesson: Need to improve efficiency of monitoring

Fundamental Questions/Challenges

- Complexity of the infrastructure
  - Distributed network
  - Heterogeneous platforms
  - Heterogeneous applications
  - Hard to detect all attacks

- Goals:
  - Associate alerts with incidents
  - Understand reasons for missed incidents
  - Propose new defense strategies
  - Analyze costs vs. benefits tradeoffs of new detection mechanisms

Detection Tools

- Bro IDS: Protocol-based detection
- NetFlow: Network traffic analysis
- Simple Event Correlator (SEC): rule-based detection

Key Findings

- Incident types
- Severity of Incidents Across Different Monitoring Tools

Example Incidents

- Enhanced malware detection tools
- Many incidents use malware to penetrate the system
- 29% of the incidents are caused by undetected malware

- Multifactor authentication system
- 22% of the incidents are caused by credential compromise

- Timely Software Update
- 9% of the incidents involve outdated applications

Possible Solutions

- Enhanced malware detection tools
- Many incidents use malware to penetrate the system
  - 29% of the incidents are caused by undetected malware

- Multifactor authentication system
  - 22% of the incidents are caused by credential compromise

- Timely Software Update
  - 9% of the incidents involve outdated applications

Related Work/Interaction with Other Projects


www.itil.illinois.edu