Insider Threats
People-Process-Control

Nabeel Mohamed
9/29/2009
WE HAVE MET THE ENEMY AND HE IS US.
Outline

- Insider threat – introduction & exploration
- Modeling insider threat behavior
- Best practices
- Insider threat detection in database systems
- Discussion
Some general definitions found in the web...

“An individual who has *special knowledge or access to confidential information*”

“A person who has *inside information about an organization*”

“A company's *officers, directors and any beneficial owners of more than ten percent of a class of the company's equity securities*” (definition of an insider for insider trading frauds)

“An individual who has access to *non-public information*”
Who is an “Insider”? 

- In information security domain...
- An individual currently or at one time authorized to access an organization’s information system, data, or network
- Implies a degree of trust in the individual
- Is it possible to design a system without trusted people?
- Can we replace trusted people with machines?
Who is a "Malicious Insider"?

- Trusted-insider-turned-malicious
- CERT Definition:
  A current or former employee, contractor, or business partner who
  - has or had authorized access to an organization’s network, system, or data and
  - intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems

(Image credit: CERT)
Malicious Insiders

- Have a significant advantage over outsiders who might want to harm an organization
- Can **bypass** physical and technical security measures designed to prevent unauthorized access
- Aware of the **policies, procedures, and technology** used in their organizations, and also often **their vulnerabilities**, such as loosely enforced policies and procedures or exploitable technical flaws in networks or systems
- Where do we draw the line for the organizational boundary?
Collusion with outsiders

“Half of the insiders who stole or modified information for financial gain were actually recruited by outsiders, including organized crime and foreign organizations or governments “

Business partners

“Increased insider crimes by employees of trusted business partners who have been given authorized access to their clients’ networks, systems, and data” (Co-operatators Life Insurance case – 2003, a call center stealing Symantec customer data case - 2009)

IT Outsourcing is a $23 billion industry in 2007
Mergers and acquisitions

“Increased risk of insider threat both within the acquiring organization, and in the organization being acquired, as employees endure stress and an uncertain organizational climate “

Cloud computing?

- One-stop access to multiple organizational data
- No physical boundaries (different countries have different policy/legal frameworks)
How bad is the insider threat?
2007 e-Crime Watch Survey

- Percentage of Participants Who Experienced an Insider Incident (671 respondents)
Consequences of Insider Incidents

- Financial losses
- Operational impact
- Damage to reputation
- Harm to individuals
- Risks to public safety and national security
Major research efforts

- CERT
  - http://www.cert.org/insider_threat/
- I3P (The Institute for Information Infrastructure Protection)
- PERSERECC (The Defense Personnel Security Research Center)
Types of Insider Threats

- IT Sabotage
- Theft or modification for financial gain
- Theft or modification for business advantage
- Insider Espionage (see Appendix)
- Miscellaneous

Discussion is mainly based on incidents collected by CERT as follows

- About 100 cases during 2003 – 2007
- About 90 cases during 1996 - 2002
Insider Threat: IT Sabotage

- Current or former employees, contractors, or business partners intentionally exceeded or misused an authorized level of access to networks, systems, or data with the intention of harming a specific individual, the organization, or the organization’s data, systems, and/or daily business operations

- Mostly former employees
- Held highly technical positions
- Disgruntled due to unmet expectations
- Outside of working hours

(Image credit: CERT)
Case: IT Sabotage

- Rajendrasinh Makwana was a UNIX contractor for Fannie Mae. On October 24, he was fired. Before he left, he slipped a logic bomb into the organization's network. The bomb would have "detonated" on January 31. It was programmed to disable access to the server on which it was running, block any network monitoring software, systematically and irretrievably erase everything -- and then replicate itself on all 4,000 Fannie Mae servers. Court papers claim the damage would have been in the millions of dollars, a number that seems low. Fannie Mae would have been shut down for at least a week (but fortunately detected before detonation)

http://www.wired.com/threatlevel/2009/01/fannie/
Insider Threat: Theft or modification for financial gain

- **Current or former** employees, contractors, or business partners **intentionally** exceeded or misused an authorized level of access to networks, systems, or data with the intention of **stealing or modifying confidential or proprietary information** from the organization for **financial gain**

- Mostly current employees
- Held non-technical positions
- Authorized access, own ID’s
- Inside working hours
- Long term attacks
- PII’s and CI’s

(Image credit: CERT)
General Cases: Theft or modification for financial gain

- An outsider recruiting an insider in a low-paying, non-technical position who has access to Personally Identifiable Information or Customer Information. The insider steals the information; the outsider then pays the insider and uses the information to commit fraud or identity theft.

- Some insiders were paid to modify data, for example credit histories. In some cases they were paid by people with poor credit histories, and in others by someone (like a car dealer) who would benefit from the beneficiaries’ loan approvals.
Insider Threat: Theft or modification for business advantage

- **Current or former** employees, contractors, or business partners **intentionally** exceeded or misused an authorized level of access to networks, systems, or data with the intention of stealing confidential or proprietary information from the organization with the intent to use it for a **business advantage**

- Longer term ambition than financial gain:
  - To get a new job, to use in a new job with a competing business, or to start a competing business, etc.

- Engineers/Sales/Technical
- Authorized access
- Inside working hours
- IP’s and CI’s
- Had job offer/started new biz.

(Image credit: CERT)
"Joe" started as a subcontractor. "Joe" was a very nice older gentleman. Within a year "Joe" was hired on full time and worked on some projects. As work would ebb and flow, he tried to get onto a few projects but apparently he had worn out his welcome because some projects preferred to work shorthanded rather than take him on. About the time the Request for Proposals (RFP) was released by the government, "Joe" resigned and went to work for another company in the next county. Surprisingly enough, this same company bid against his previous company on the RFP although they had no previous experience doing that sort of work or working for this government agency. Apparently they had the right answers because they were able to successfully win the RFP with a slightly lower bid. While "Joe" wasn’t named on their proposal response, he ended up having a senior position on that account...
Insider threats are real and can be damaging!

What can we do about it?

How can they be prevented/mitigated/detected?

How can we respond to insider incidents?
People-Process-Control

- Insiders have legitimate access; monitoring and controlling access alone cannot solve the insider problem
- **People** – understand the behavior of those using the information system
- **Process** – follow best practices
- **Control** – have technical controls in place to prevent/mitigate/detect/identify insider threats and respond to insider threats
~ People ~
People – behavioral modeling

- Preliminary System Dynamics Maps of the Insider Cyber-threat Problem, CERT, 2005
  - 25 researchers from 8 different institutions and representing different disciplines
  - Modeled trusted-insider-turned-malicious behavior
  - The study is old but the findings are still valid
Why behavioral modeling?

• Understanding the behavior allows
  • To develop best practices to mitigate risks associated with insider threat
  • To continue to have sufficient control in place
  • To maintain a balance between trust and monitor
Simplified systems dynamics model
The detection trap

- Explains why organizations are historically under-invested on accepted security practices at the time of insider attack
The trust trap

- Explains how well intentioned organizational activities can erode an organization’s defenses to insider threats
- Is having a high level of managerial trust a good thing?  
  - Yes and no
The Unobserved Emboldening

- Explains how attackers overcome their personal level of perceived risk, holding off on final attack behaviors until perceived risks fall to a level the attacker is willing to accept.
How can this modeling actually help mitigate insider threats?

- Understand the level of trust and empowerment
- Maintain security at an acceptable level
- Increase the level of risk awareness within the organization
- Need for better reporting systems (B. Schneier 2000)

- Bottom Line: Increased trust and increased perception of risk may lead to a better working place with minimal insider threat
The Process

Best Practices
Six common sense security best practices

1/2

• **Limit** the number of **trusted** people
  • Fewer trusted people, fewer threats
  • E.g.: fewer people have access to all the labs in the CS building, know the combination to the safe in a bank

• Ensure that the trusted people are also **trustworthy**
  • E.g.: background checks, limiting the jobs to citizens, bonding employees, prohibiting convicted felons

• **Limit the amount of trust** each person has
  • Limits the damage caused by an individual if he/she turns out to be not trustworthy
  • E.g.: My key is programmed to open only 2161 lab

http://online.wsj.com/article/SB123447990459779609.html
Six common sense security best practices

[2/2]

• Give people **overlapping spheres of trust**
  • Makes it much harder for one employee to defraud the system
  • E.g.: Two signatures on corporate checks over a certain value, two people with two separate keys to launch nuclear missiles

• **Detect** breaches of trust after the fact and **prosecute** the guilty (audit is so vital)
  • Punishing perpetrators in public increase the deterrence effect (increase in perceived risk by insiders)

• Keep employees **happy 😊**

http://online.wsj.com/article/SB123447990459779609.html
Insider attack detection in RDBMS
The discussion is mainly based on the following two papers:


Papers
Intrusion Detection (ID)

- An IDS detects unwanted attempts at accessing, manipulating, and/or disabling a target
- Unauthorized access (mainly from outside)
  - An outsider masquerades/impersonates as a legitimate user
- Three main types
  - Network
  - Host
  - Application (our focus)
ID techniques

• Misuse detection
  • Keeps profiles of intrusive patterns
  • Identifies behavior patterns characteristic of intrusions

• Anomaly detection
  • Keeps/builds profiles of normal patterns
  • Identifies anomalous behavior patterns (deviations from the normal behavior)
Anomaly detection

• Many statistical approaches available
• Why does it work?
  • A masquerader has stolen someone’s credentials
  • They can access what the victim is authorized to use
  • But they are unlikely to perform actions consistent with the victim’s typical behavior
  • Behavior is not something that can be easily stolen!
• Can we use the same techniques to detect insider attacks?
<table>
<thead>
<tr>
<th>Intrusions</th>
<th>Insider attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outsider</td>
<td>Malicious insider</td>
</tr>
<tr>
<td>Masquerade</td>
<td>Masquerade/traitor (same as the malicious insider)</td>
</tr>
<tr>
<td>Unauthorized</td>
<td>Authorized</td>
</tr>
<tr>
<td>Outside organization’s perimeter security</td>
<td>Inside or outside organization’s perimeter security</td>
</tr>
<tr>
<td>May not be aware of the policies, procedures, and technology used organizations, and also often their vulnerabilities</td>
<td>Usually aware of the policies, procedures, and technology used organizations, and also often their vulnerabilities</td>
</tr>
<tr>
<td>Mostly technical</td>
<td>Technical or non-technical</td>
</tr>
<tr>
<td>Mostly anomalous</td>
<td>May or may not be anomalous</td>
</tr>
</tbody>
</table>
Insider attack detection (IAD) [1/2]

- How are they currently detected by organizations?
  - Notification of a problem by a customer
  - Law enforcement officer, coworker, informant, auditor, or other external person who became suspicious
  - Sudden appearance of a competing business
  - Unable to perform daily operations
  - Accidental discovery during system/configuration upgrades

- How the insider identified after detection?
  - Mostly through various logs
  - Can organizations do better?
Two class of individuals
- Masqueraders (using the stolen credentials of a coworker)
- Traitor (using own credentials)
A disgruntled may act as either of them
What techniques exist in the literature to detect insider attacks?
- User profiling for anomaly detection
- Trap-based defense mechanisms (honeypots) to attract malicious insiders
IAD in RDBMS – Two approaches

- A good IAD should be
  - **Useful** – able to *correctly* detect a large class of insider attacks
  - **Practical** – able to perform *effectively* in a real RDBMS
- Syntax-centric approach [Kamra et. al. 2008]
  - Profile **SQL queries** and detect deviations
- Data-centric approach [Mathew et. al. 2009]
  - Profile **query results** and detect deviations
- Both are only effective for masqueraders and traitors who deviates significantly from the normal profiled behaviors
Syntax-centric approach

- Key idea
  - Extract access patterns from SQL queries
  - Build profiles at different granularity levels
    - Build profiles per role
    - Train a classifier with role as the class
    - Declare a request as anomalous if classifier predicted role does not match the actual role

Note: The paper talks about an unsupervised learning approach as well.
Example: coarse-grained profile [1/4]

**Schema**

T1 : {a1,b1,c1}  
T2 : {a2,b2,c2}  
T3 : {a3,b3,c3}

**Query**

SELECT T1.a1, T1.c1, T2.c2 FROM T1, T2, T3  
WHERE T1.a1 = T2.a2 AND T1.a1 = T3.a3

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>SELECT</td>
</tr>
<tr>
<td>Num Projection Tables</td>
<td>2</td>
</tr>
<tr>
<td>Num Projection Columns</td>
<td>3</td>
</tr>
<tr>
<td>Num Selection Tables</td>
<td>3</td>
</tr>
<tr>
<td>Num Selection Columns</td>
<td>3</td>
</tr>
</tbody>
</table>
Example: medium-grained profile [2/4]

**Schema**

<table>
<thead>
<tr>
<th>T1</th>
<th>T2</th>
<th>T3</th>
</tr>
</thead>
<tbody>
<tr>
<td>{a1,b1,c1}</td>
<td>{a2,b2,c2}</td>
<td>{a3,b3,c3}</td>
</tr>
</tbody>
</table>

**Query**

```
SELECT T1.a1, T1.c1, T2.c2 FROM T1, T2, T3
WHERE T1.a1 = T2.a2 AND T1.a1 = T3.a3
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>SELECT</td>
</tr>
<tr>
<td>Projection Tables</td>
<td>[1 1 0]</td>
</tr>
<tr>
<td>Projection Columns</td>
<td>[2 1 0]</td>
</tr>
<tr>
<td>Selection Tables</td>
<td>[1 1 1]</td>
</tr>
<tr>
<td>Selection Columns</td>
<td>[1 1 1]</td>
</tr>
</tbody>
</table>
Example: fine-grained profile [3/4]

**Schema**

| T1 : {a1,b1,c1} | T2 : {a2,b2,c2} | T3 : {a3,b3,c3} |

**Query**

```
SELECT  T1.a1, T1.c1, T2.c2 FROM T1, T2,T3  
WHERE  T1.a1 = T2.a2 AND T1.a1 =T3.a3
```
Data: \{\text{Cmd, NumProjTabs, NumProjCols, NumSelTabs, NumSelCols}\}
Learn \(P(\text{Cmd} | R), P(\text{Cmd} | \neg R), P(\text{NumProjTabs} | R), \text{etc}\)
Predict \(P(R | \text{Cmd, NumProjTabs, .., NumSelCols})\)
\[= P(\text{Cmd, NumProjTabs, .., NumSelCols} | R)P(R) \]
\[= P(\text{Cmd} | R) \ldots P(\text{NumSelCols} | R)P(R) \]
If predicted \(R \neq \text{actual } R \Rightarrow \text{suspicious action}\)
Two syntactically similar queries may generate vastly different results:

SELECT p.name FROM Product p WHERE p.price == 5
SELECT p.name FROM Product p WHERE p.price != 5
(quick remedy: profile predicate operations and values)

Attributes may not be conditionally independent:
(quick remedy: model dependencies in Bayesian nets)

Two syntactically distinct queries may generate similar results:
SELECT p.name FROM Product p WHERE p.price != 5
SELECT p.name FROM Product p WHERE p.price < 5 AND p.price > 5
Data-centric approach

- **Key idea**
  - Extract statistical patterns from query results
    - Numeric attributes (min, max, mean, median, std)
    - Non-numeric attributes (#count, #distinct)
  - Build profiles for roles (NBC, DT, SVM) based on result schemas and statistical patterns (S-Vector)
    - Declare a request as anomalous if classifier predicted role does not match the actual role
Example: S-Vector

- SELECT p.cost, p.type FROM Product p WHERE p.cost < 1000;

<table>
<thead>
<tr>
<th>S-Vector Features</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product.type.ncount</td>
<td>50</td>
</tr>
<tr>
<td>Product.type.ndistinct</td>
<td>10</td>
</tr>
<tr>
<td>Product.cost.Min</td>
<td>5</td>
</tr>
<tr>
<td>Product.cost.Max</td>
<td>980</td>
</tr>
<tr>
<td>Product.cost.Mean</td>
<td>380</td>
</tr>
<tr>
<td>Product.cost.Median</td>
<td>405</td>
</tr>
<tr>
<td>Product.cost.StdDev</td>
<td>55</td>
</tr>
</tbody>
</table>
Issues/Improvements

- Query execution is necessary to detect anomalies (Quick remedy: maintain stats at table level – instead of the query result – query for stats)
- Possible inference attack #1 (paper mentions this)
  
  ```sql
  SELECT * FROM Product p WHERE p.cost < 1000;
  SELECT * FROM Product p WHERE 1;
  ```

  If the second query is allowed based on the first one, the attacker can infer that all prices are less than 1000

- Possible inference attack #2
  
  Only allowed to access the following view:
  
  ```sql
  CREATE VIEW EmployeeV AS SELECT e.name FROM EMPLOYEE;
  SELECT ev.name FROM EmployeeV ev, Employee e WHERE ev.name = e.name ORDER BY e.salary DESC;
  ```

  Still retrieves only names but they are ordered.
Discussion [1/3]

- IAD in RDBMS – third approach?
  - What if we compare query plans instead
- Insider attacks may exhibit normal behavior
  - Won’t be able to detect by anomaly based ID approach
  - How can we capture the intent/context of insider? Can profiling insider search behavior help in this?
  - Can we use auxiliary background information to better at prediction? (location, time of day, session duration, frequency, sending an email after a search, etc.)
- Can we design trapping systems without hindering legitimate operations but attract traitors to believe they are real? (There isn’t much research for insider threats)
Discussion [2/3]

- Insider attacks may have been planned/executed for a longer period (months or a couple of years)
  - These attacks may be incremental in nature
  - How can we detect such attacks at the initial stage before becoming damaging?
- Legal issues
  - How can an insider be challenged when detection system identifies a malicious activity?
- Privacy issues
  - How can the admin be alerted about a possible attack without revealing insider identity until the attack has been validated?
  - What is the acceptable level of monitoring?
Discussion [3/3]

- Fine-grained access control in DBMS?
  - Cell-level access control
  - Hippocratic databases
  - Predicated grants, etc
- Can we use social networks such as Facebook, Twitter, blogs, etc. to identify possible threats? (Is it ethical?)
- Most of the research work use synthesized data for experiments
  - Do they reflect the real data?
  - Even if available, what types of audit sources are most discriminatory to reliably detect insider malicious behavior?
Acknowledgement

- Some materials in this presentation are borrowed from publicly available slides. Mainly from:
References [1/2]

- Combating the Insider Cyber Threat, IEEE Security & Privacy, Jan/Feb 2008
- Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis, TR CERT, 2006
- Preliminary System Dynamics Maps of the Insider Cyber-threat Problem, CERT Research Proposal
References [2/2]

- Data Theft: A Prototypical Insider Threat, Michael McCormick, In Insider Attack and Cyber Security 2008
- Detecting Anomalous Access Patterns in Relational Databases, Ashish Kamra, Evimaria Terzi, Elisa Bertino, VLDB Journal 2008
Appendix
Case: IT Sabotage

S.F. officials locked out of computer network - July 2008:
A disgruntled city computer engineer, Terry Childs (basic salary over $125K), has virtually commandeered San Francisco's new multimillion-dollar computer network, altering it to deny access to top administrators even as he sits in jail on $5 million bail, authorities said Monday....he had been disciplined on the job in recent months for poor performance and that his supervisors had tried to fire him...They weren't able to do it - this was kind of his insurance policy...As part of his alleged sabotage, Childs engineered a tracing system to monitor what other administrators were saying and doing related to his personnel case...he has been charged with four counts of computer tampering...

http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/14/BAOSuPvM5.DTL
Espionage Cases

• Are they considered insider threats?
  • Could be done by insiders or outsiders
• Insiders may spy for foreign governments
  • Insider espionage threat
• According to the PERSEREC study, one-third of all espionage against the U.S. since 1945 was conducted by persons with security clearances who worked in either the intelligence or communications fields
ANDERSON, RYAN GILBERT, 26, a Specialist and tank crewman in the Washington National Guard, was arrested on 12 February 2004, and charged with five counts of attempting to provide aid and information to the enemy, Al Qaeda... In late 2003, as his National Guard unit was preparing to deploy to the war in Iraq, Anderson went onto Internet chat rooms and sent emails trying to make contact with Al Qaeda cells in the United States... in late January 2004, Anderson was videotaped offering to persons he thought were Al Qaeda operatives, sketches of M1A1 and M1A2 tanks, a computer disk with his identifying information and photo, and information about Army weapons systems....

New York Times 13 Feb 2004, “Guardsman Taken Into Custody and Examined for Qaeda Tie”
The PERSEREC report ESPIONAGE CASES 1975-2004, Summaries and Sources
## Comparison of Attacks (CERT case study) [1/2]

<table>
<thead>
<tr>
<th></th>
<th>Insider IT Sabotage</th>
<th>Insider Theft or Modification of Information for Financial Gain</th>
<th>Insider Theft of Information for Business Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage of crimes in CERT’s case database</td>
<td>45%</td>
<td>44%</td>
<td>14%</td>
</tr>
<tr>
<td>Current or former employee?</td>
<td>Former</td>
<td>Current</td>
<td>Current</td>
</tr>
<tr>
<td>Type of position</td>
<td>Technical (e.g. system administrators or database administrators)</td>
<td>Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)</td>
<td>Technical (71%) - scientists, programmers, engineers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sales (29%)</td>
</tr>
<tr>
<td>Gender</td>
<td>Male</td>
<td>Fairly equally split between male and female</td>
<td>Male</td>
</tr>
<tr>
<td>Target</td>
<td>Network, systems, or data</td>
<td>Personally Identifiable Information or Customer Information</td>
<td>Intellectual Property (trade secrets) – 71%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Customer Information – 33%</td>
</tr>
</tbody>
</table>
## Comparision of Attacks (CERT case study) [2/2]

<table>
<thead>
<tr>
<th></th>
<th>Insider IT Sabotage</th>
<th>Insider Theft or Modification of Information for Financial Gain</th>
<th>Insider Theft of Information for Business Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access used</strong></td>
<td>Unauthorized access</td>
<td>Authorized access</td>
<td>Authorized access</td>
</tr>
<tr>
<td><strong>When</strong></td>
<td>Outside normal working hours</td>
<td>During normal working hours</td>
<td>During normal working hours</td>
</tr>
<tr>
<td><strong>Where</strong></td>
<td>Remote access</td>
<td>At work</td>
<td>At work</td>
</tr>
<tr>
<td><strong>Recruited by outsiders</strong></td>
<td>None</td>
<td>Half recruited for theft; less than one third recruited for modification</td>
<td>Less than one fourth</td>
</tr>
<tr>
<td><strong>Collusion</strong></td>
<td>None</td>
<td>Almost half colluded with another insider in modification cases; 2/3 colluded with outsiders in theft cases</td>
<td>Almost half colluded with at least one insider; half acted alone</td>
</tr>
</tbody>
</table>
From the most recent CERT case study [1/3]

- Break down of 190 insider threat cases

Note: Includes about 100 cases in 2003 – 2007 and the rest 1996 - 2002
Overlap among the insider threat cases
Distribution of cases by critical infrastructure sector:
Insider theft of intellectual property for business advantage: A preliminary model, CERT, MIST 2009
Introduction

- Group modeling and analysis of 35 cases of insider theft of IP
- Intention – take to a new job, get a new job, start a competing business
- The paper describes two scenarios
  - The entitled independent scenario (we look at only this)
  - The ambitious leader scenario
Increased feeling of entitlement led to less perceived risk by the individual even when an IP agreement has been signed.
Dissatisfaction leading to compromise

- Entitlement acts as a catalyst
Entitled individual rarely acts as if they doing something wrong.
1. Consider threats from insiders and business partners in enterprise-wide risk assessments
2. Clearly document and consistently enforce policies and controls
3. Institute periodic security awareness training for all employees
4. Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process
5. Anticipate and manage negative workplace issues
6. Track and secure the physical environment
7. Implement strict password and account management policies and practices
8. Enforce separation of duties and least privilege
16 CERT Best Practices [2/2]

9. Consider insider threats in the software development life cycle
10. Use extra caution with system administrators and technical or privileged users
11. Implement system change controls
12. Log, monitor, and audit employee online actions
13. Use layered defense against remote attacks
14. Deactivate computer access following termination
15. Implement secure backup and recovery processes
16. Develop an insider incident response plan