The Threat of the Insider Threat

Matt Bishop

Dept. of Computer Science

University of California at Davis

Disclosure

I have no relevant financial interest,
arrangements,
or affiliation with
any organizations related to
commercial products or services
to be discussed at this program

Others Who Contributed

- Dr. Carrie Gates, CA Labs
- Dr. Sean Peisert, UC Davis and LBNL
- Prof. Sophie Engle, USF (and as a student at UC Davis)
- Dr. Sean Whalen, UC Davis (and as a student at UC Davis)

Outline

- Overview
- What is the insider?
- Definitions and problems with them
- Common elements and what we can learn
- How do we use this?
- Conclusion

Overview

- Government intelligence analyst
  - By day: analyzes information obtained from monitoring electronic signals to determine what adversary is up to
  - By night: provides this information to the adversary so they know what the analyst's government is being told

Legendary Example

- Greeks wanted to get inside Troy
- They built a horse and put soldiers inside
- The Trojans pulled the horse into the city
- At night, the Greeks inside the horse got out and opened the gates
- The Greeks entered the city (and sacked it)

Real-Life Examples

- In World War II, Abwehr sent spies to England
  - Germany fed them information about other spies
  - British had captured all of them, turned many of them, and so got the information
- But Soviets had penetrated British counter-intelligence
  - Kim Philby was high-ranking British official
  - He was also a Soviet spy

Defining the Insider

- "an already trusted person with access to sensitive information and information systems"
  - *Understanding the Insider Threat*, RAND (2004), xi
- "someone with access, privileges, or knowledge of information systems and services"
  - Same report, 10
- Anyone operating inside the security perimeter
  - *New Incident Response Best Practices: Patch and Process is No Longer Acceptable Incident Response*, Guidance Software, 3

More Definitions

- “an individual who has been granted any level of trust in an information system”
- “a person with legitimate access to an organization’s computers and networks”
- “an individual with privileged access to an [information technology] system”

Still More Definitions

- "Insider attacks—that is, attacks by users with privileged knowledge about a system"
  - – "Designing Host and Network Sensors to Mitigate the Insider Threat," *IEEE Security & Privacy*
- "legitimate users in an IT Infrastructure"
  - – "Towards an Insider Threat Prediction Specification Language," *Information Management & Computer Security*

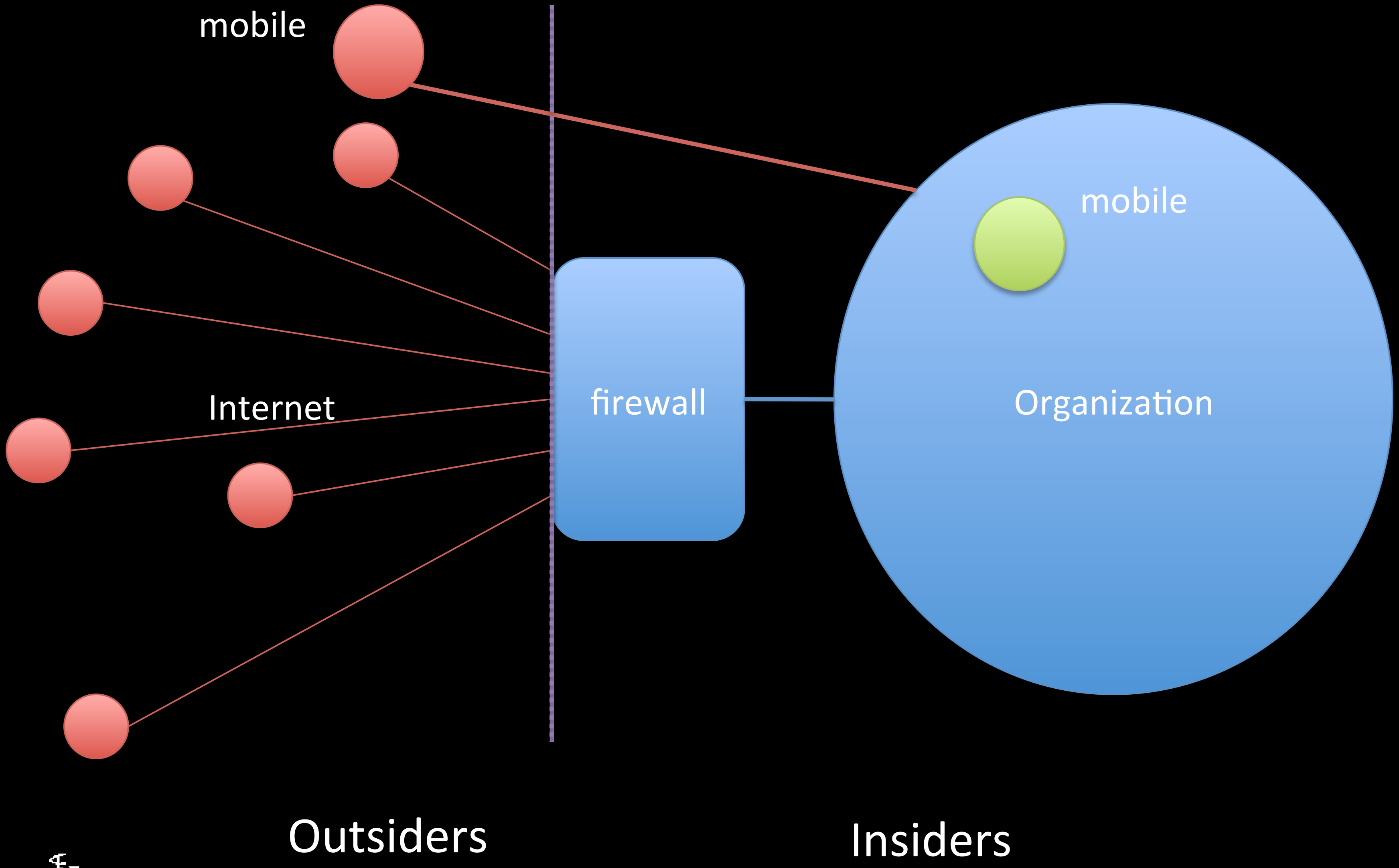
And Still More Definitions

- “a person [who] has been legitimately empowered with the right to access, represent, or decide about one or more assets of the organization's structure”
- “a human entity that has/had access to the information system of an organization and does not comply with the security policy of the organization”

And a Final Definition

- "A current or former employee, contractor, or business partner who
  - has or had authorized access to an organization's network, system 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"
    - *Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition — Version 3.1*, 5

Perimeters


mobile
Internet
firewall
mobile
Organization
Outsiders
Insiders

Problems

- How well defined is your perimeter?
  - Mobile computing
  - Virtual private networks
  - Remote sites
  - Unknown modems, etc.
- How does physical access play into this?
  - Authorized users
  - Others, such as janitors

Supply Chain Problem

- Someone sells you a program to solve a problem your company has
- When you use it, it copies data from your computer (including medical records) to a server on the Internet
- So . . . *Are you an insider?*
- And . . . *Is the person who wrote it an insider?*
- And . . . *Is the person who sold it an insider?*

Not Just Computer Scientists

- Insider trading
  - In U.S. law, defined by the agency that regulates the stock exchanges (Securities Exchange Commission)
  - Extensively litigated over the years
  - Considerable grey area makes it difficult to know whether particular transaction is legal or not

Common Notions in Definitions

- *Access*
  - Without access, nothing can happen
  - Access can be *direct* or *indirect*
- Hunker, Probst list 4 categories of attributes of insiders
  - Knowledge
  - Ability to represent something
  - Trust by the organization
- All require some form of access

What Controls Access?

- Security policy
- Security mechanisms
- The mechanisms are *imprecise*

Our Approach

- Apply notion of "layers of abstraction" to security policy
- Examine the discrepancies between different layers
- Can integrate intention into these layers

Issues

- Feasibility
  - Computer systems understand *accounts*, not *people*
  - Computer systems understand *actions*, not *intentions*

Example

- Policy: *Alice is authorized to read medical records for the purpose of computing statistics*
- Implementation: *account alice is authorized to read files labeled "medical records"*
- GAPS
  - Anyone with access to account *alice* can read files labeled "medical records"
  - Account *alice* can read medical records and then do anything with that data (including selling the data)
  - Account *alice* can read any file labeled "medical record" whether it is a medical record or not

Unifying Policy Hierarchy

Level	Domain	Description
Oracle Policy	All possible (*s*, *o*, *a*, *e*) tuples	Captures notion of “ideal policy” even if not explicitly defined
Feasible Policy	System-definable (*s*, *o*, *a*, *e*) tuples	Represents the policy as it can be captured on an actual system
Configured Policy	System-definable (*s*, *o*, *a*, *e*) tuples	Represents the policy as configured on an actual system
Real-Time Policy	System-definable (*s*, *o*, *a*, *e*) tuples	Represent the policy implemented on an actual system

s subject, *o* object, *a* action
e environment (including intent, if appropriate)

The Threats

- Consider these threats
  - Someone has *more* access at lower policy level than at higher policy level
  - Someone has *less* access at lower policy level than at higher policy level
    - We don’t discuss this further here
- Side note: these seem to map onto what others consider an “insider”

Examples Between Levels

- Oracle/Feasible: social engineering, covert channels
- Feasible/Configured: not eliminating ex-employees' privileges
- Configured/Real-Time: programs with vulnerabilities that lead to escalation of privileges

Detailed Example

- Bob surfing web using browser vulnerable to remote exploit
- Accidentally surfs to site with attack that exploits it
  - If attacker, Alice, gets access to Bob’s account, she’s in the Configured/Real-Time gap
- Deliberately surfs to site with attack that exploits it; claims “oops, I didn’t know!”
  - Now Bob gives access to Alice, so he’s in the Oracle/ Feasible gap

Assumption for Talk

- In what follows, assume system configured correctly
  - That is, Feasible Policy = Configured Policy
- Two primitive actions for this type of attack:
  - Violation of Oracle Policy using access granted by Configured Policy
  - Violation of Configured Policy using access granted by Real-Time Policy

Key Point

- Other definitions give rules, descriptions of who is an insider
  - You are either an insider or you aren't
- This allows degrees of "insiderness"
  - Partial ordering
  - Also handles physical security considerations
  - Note: model does *not* define "insider"; you can draw a line (or area) anywhere you deem appropriate to divide the attackers into insiders and outsiders

Finding the Attackers

- Previous example: discrepancy between access of *individual* Alice and *account* alice
- So, we model access

ABGAC

- Access-Based Group Access Control
- Generalizes RBAC
  - RBAC focuses on *roles*, or job functions
  - ABGAC focuses on attributes that may, or may not, be related to job function
  - Example: janitor has access to computer room after 5PM; can pull plugs on servers
    - No relationship between job and computers, officially
    - Relationship between access and computers, though

Example

- Sam, Robin married; Sam owns company whose stock will rise tomorrow
  - If Sam advises Robin to invest, clear conflict of interest
- RBAC: separation of duty fails as Robin has no job relationship to the company
- ABGAC: define 2 groups, rule saying members of second group cannot perform actions that members of first group can
  - Sam in first group, Robin in second group

Applying to Insiders

- Basic idea
  - Define groups of resources
  - Define groups of users
  - Define modes of access of interest
- Additional ideas
  - Devise measures of risk for user, resource groups
  - Use these, and proximity, to calculate risk and cost of compromise
  - Focus on those that concern you the most

What To Worry About

- Which assets (resources, information) are important to *you*?
- Which are importan to the *attacker*?

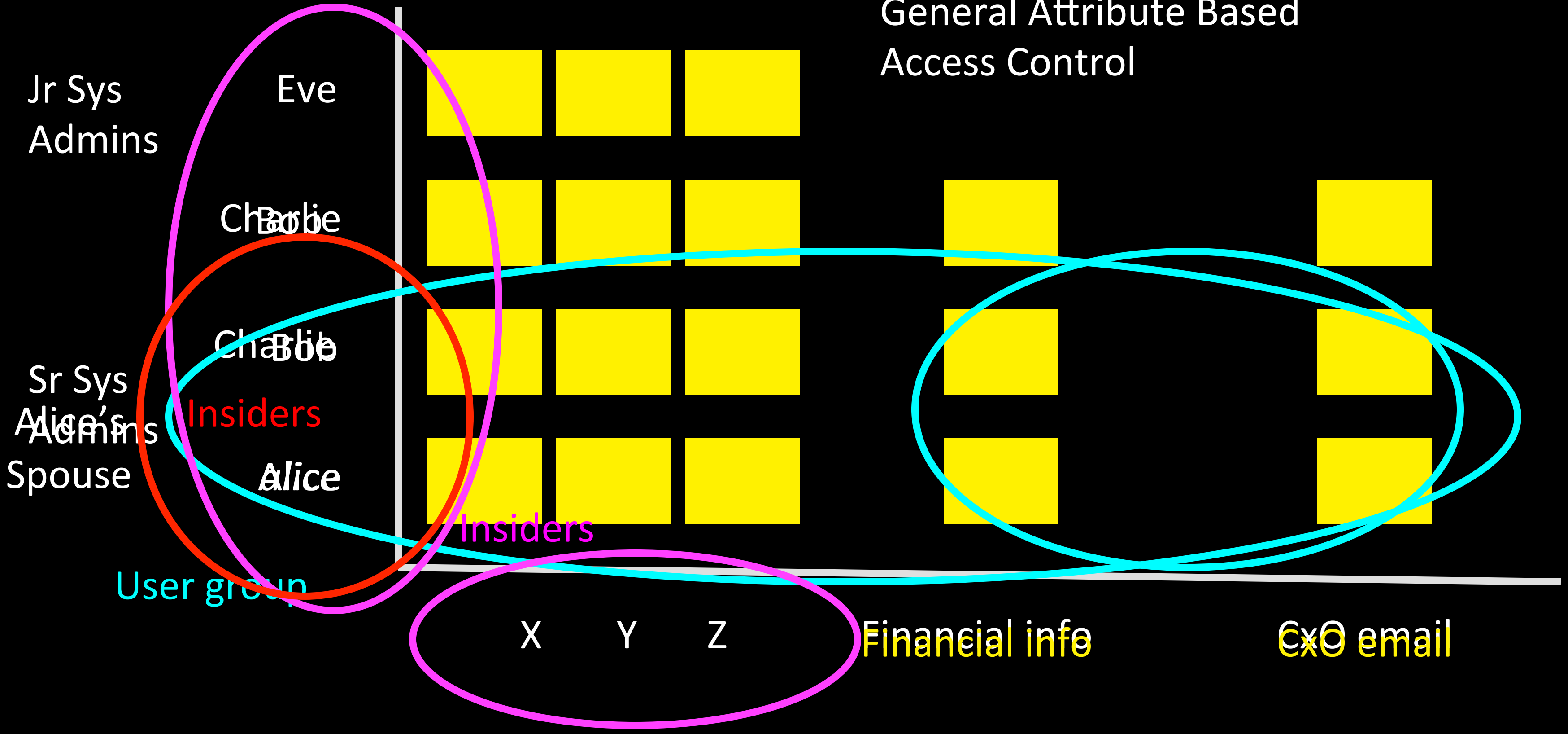
Components

- *Resource pair*: (resource/entity, access mode)
  - (printer, write)
  - (printer, remove)
- *Resource domain*: $rd = \{ (r_1 , a_1), \ldots, (r_n, a_n) \}$
  - Idea: set of ways resource can be accessed
  - Example use: covert channel; one resource pair for reading channel, another for manipulating it

Components

- *Rd-group*: set of resource domains
  - Idea: insider attacks need access to multiple resource domains
  - Read data from one domain, write it to another to transmit it
- *User group*: set of subjects whose protection domains are superset of associated rd-group
  - These are the potential attackers

General Attribute Based Access Control



Resource pair

Resource domain

rd-group

Read access

Read access

Physical access

Write access?

Certain desktops

Certain desktops

Certain laptops

Certain backups

Certain printers

Example: E-Voting

- Oracle policy: access to electronic voting systems restricted to election officials
  - Easy to enforce: lock up until used
  - In practice: sleepovers
- Question: who are the insiders?
  - rd-group: e-voting systems sleeping over, physical access
  - User groups: includes all who have physical access to systems at poll worker's house
    - Family members, burglars, etc.
  - Feasible policy ≠ Oracle policy

Developing Groups

- Determine important components relevant to privilege of interest
  - Management must do this with help of technical folks
  - Ask: what resources are needed, how would they be used, to compromise system
- Determine user groups who have same access
  - Go beyond “cyber” access to consider physical access and social access (in essence, compute transitive closure)

Observations

- Can define "proxy users"
  - Then expand these into user groups as needed
- Analyze policies, procedures to enforce security
  - Appropriate: firing after the fact won't help information leak
  - Enforceable: touching system not enforceable unless monitored around the clock

Psychological and Social

- Whom do you want to worry about?
- Psychosocial influences

Put These Together

- Determine who has access to a resource
- Determine what access each person has
- Result: user groups associated with rd-group
- Then define appropriate cost function
- Build lattice
- Iterate, adding in types of access not yet captured
- Make decisions

Example: E-Recordation

- Goal: recording real estate over the Internet
  - Integrity, accountability critical here
- Company is US-based
  - Developers in the Ukraine, Nicaragua, U.S.
  - Software development servers in Iowa, U.S.
- Problem: identify attackers who may create trap doors during development that allow modification of data after parties all sign it
- Note: what follows is ***simplified***!!!

Resources

- Developers work on home systems, upload software to servers using VPNs
  – Developer systems
  – VPN
  – Server
  – Backup media
- Management most concerned with illicit modification of software, so focus on that

Resource Groups

- Backup media (bkp) resource group:

  rdBKP = { (bkp,write), (bkp,remove), (bkp,destroy) }

- Servers (svr) resource group:

  rdSVR = { (svr, write), (svr, connect), (svr, login) }

- VPN resource group:

  rdVPN = { (vpn, configure) }

- Developer workstation (dws) resource group:

  rdDWS = { (dws, login), (dws, modify), (dws, download) }

User Groups

- For rd-group rdDWS (developer workstation):
  - Developers have needed access (obviously)
    - Work from home, so dws at home
    - Access VPN using dongle
  - Developer's family/other who live in home
  - People with access to the home and opportunity to tamper with computer
  - Computer repair technicians
    - Access restricted by time
  - People with electronic access to computer
    - Rogue web sites …

Risk Analysis

- Two measures of interest to management:
  - Value of programs developed
    - So must protect all backup media
  - Value of particular employee
    - Senior managers (SM), sysadmins (SA) most valuable; then developers (D); then physical maintenance folks (janitors) (PM)
- *c*'s range: pair:

  (effect of person attacking, value of resource)
- Example: analyze with respect to backups

Some Users

- Tom: system administrator with access to backups, servers
  - (SA, { bkp, svr })
- Kolya: developer living in Moscow with access to development workstation, servers
  - (D, { dws, svr })
- Judy: president with access to backups
  - (SM, { bkp })

Some More Users

- Angie: janitor sweeping out machine room
  - (PM, { svr })
- Natalya: Kolya’s wife
  - (D, { dws, svr })

Values of Resources

- 3 resources: bkp, svr, dws
- Assign values to each rd-group
- Example:
  - 100: { bkp, svr, dws }
  - 75: { bkp, svr }
  - 70: { bkp }
  - 60: { svr, dws }
  - 50: {svr}

Combining These

- Risk for each user:
  - Risk for Tom: (3, 75)
  - Risk for Kolya: (2, 60)
  - Risk for Judy: (3, 70)
  - Risk for Angie: (1, 50)
  - Risk for Natalya: (2, 60)
- Notes:
  - Corrupt sysadmins more dangerous than corrupt executives
  - if backups stored in server room, Angie’s risk is (1, 75)

Future Work

- How do you determine threats?
  - Better logging using goal-based approach
- How do we gather, analyze psychosocial information?
  - And what about privacy?
- Expand hierarchy of policy abstractions
  - Broaden notion to capture "vulnerabilities" in general
- Examine insiders by omission
  - Rather than defining insiders by additional privileges in lower layer, define them by *reduced* privileges in lower layer

Conclusion

- Treat attackers as a continuum, not as binary "inside" and "outside" divisions
- Introduced ABGAC, a model of access control based on "groups" rather than "roles"
  - Focuses on what is *possible* rather than what is authorized

‘TIME-TRAVELER’ BUSTED FOR INSIDER TRADING
Wednesday March 19, 2003

By CHAD KULTGEN

NEW YORK — Federal investigators have arrested an enigmatic Wall Street wiz on insider-trading charges — and incredibly, he claims to be a time-traveler from the year 2256!

Sources at the Security and Exchange Commission confirm that 44-year-old Andrew Carlssin offered the bizarre explanation for his uncanny success in the stock market after being led off in handcuffs on January 28.

“We don't believe this guy's story — he's either a lunatic or a pathological liar,” says an SEC insider.

“But the fact is, with an initial investment of only $800, in two weeks’ time he had a portfolio valued at over $350 million. Every trade he made capitalized on unexpected business developments, which simply can't be pure luck.

“The only way he could pull it off is with illegal inside information. He’s going to sit in a jail cell on Rikers Island until he agrees to give up his sources.”

…

— *Weekly World News*

Author Information

Matt Bishop
Dept. of Computer Science
University of California at Davis
1 Shields Ave.
Davis, CA 95616-8562

Phone: (530) 752-8060
Email: bishop@cs.ucdavis.edu
WWW: http://seclab.cs.ucdavis.edu/~bishop