Detecting Insider Attackers

Angelos D. Keromytis
Network Security Lab
Department of Computer Science

Introduction

- The insider problem is one of the oldest and toughest problems for any organization
  - E.g. military, governments, and financial institutes
  - Probably a psych problem, but network is target rich

- Not the most common, but perhaps the most damaging
  - E.g. Damage > $7.2B at Societe Generale [Bren08]

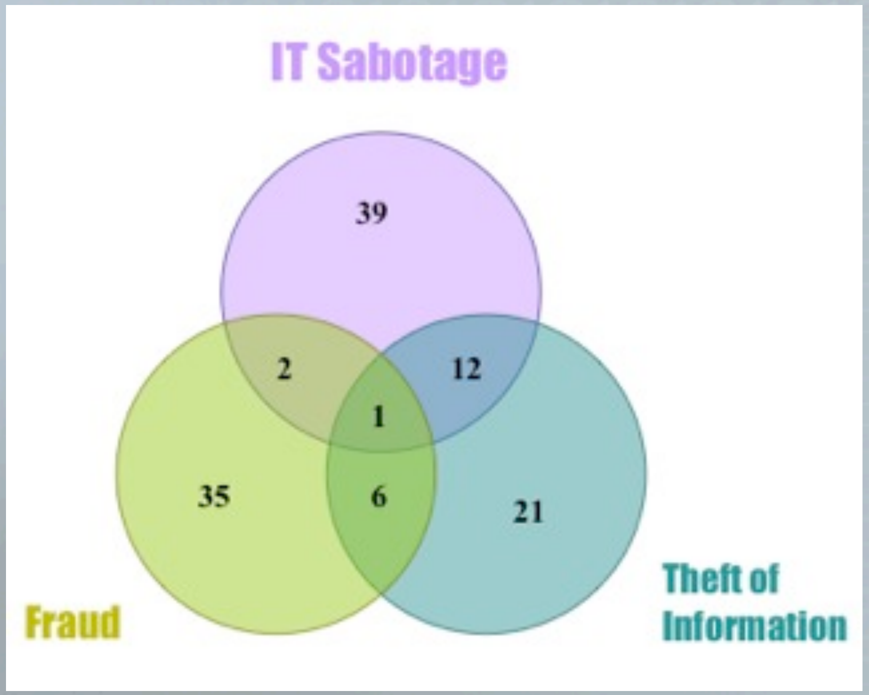
- Focus will be on insider threat and various defense strategies
  - Emphasis on trap-based mechanisms

Outline

- Motivation: Insider threat
- Policy-based prevention strategies
  - [9, 19]
- Anomaly Detection Strategies
  - [14, 15, 16, 20, 28, 30]
- Deception in defense
  - [10, 22, 27]
- Proactive detection
  - [1, 2, 7, 8, 12, 13, 17, 23, 24, (25), 26,29]
- Evaluation methodologies
  - [11, 21]
- Wireless and VM decoys

Motivation: Insider Threat

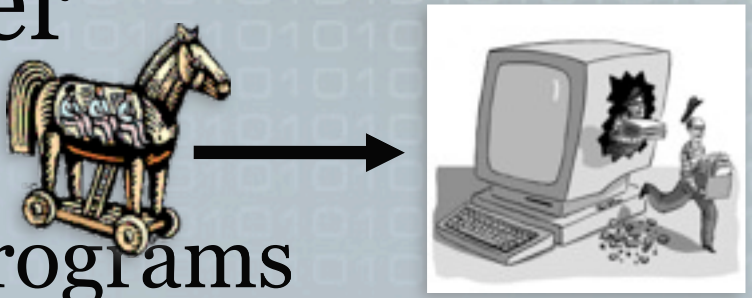
- CERT/E-Crime Watch survey[CMST06]:
  - Conducted detailed analysis of 116 insider cases
  - 20% committed by insiders
- Motive of insiders:
  - Sabotage: 54
  - Fraud (includes misuse):44
  - Theft of information:41



- Other ways to distinguish:
  - Masqueraders versus traitors
  - Levels of sophistication or knowledge (e.g., admin vs. unprivileged user)
  - Risk

Motivation: Privileged Software

- External threat acquires insider characteristics
  - Example: Spyware/Trojan Horse Programs
  - Very common



- Recent study on Zeus (largest botnet):
  - Over 3.6 million PC infections [Messmer09]
  - 55% bypassed up-to-date antivirus software [Trusteer09]
- Underground economy trading in stolen credentials has spurred the growth

Network-level Compromise

- Infiltration of the network through protocol level attacks
  - Password guessing, router hijacking, or a vulnerability in WiFi security.
  - In the case of TJX, internal access, ste [Pereira07] .
  - Only 49% of corporate access points in NYC and 48% in London used advanced security [CGV08]

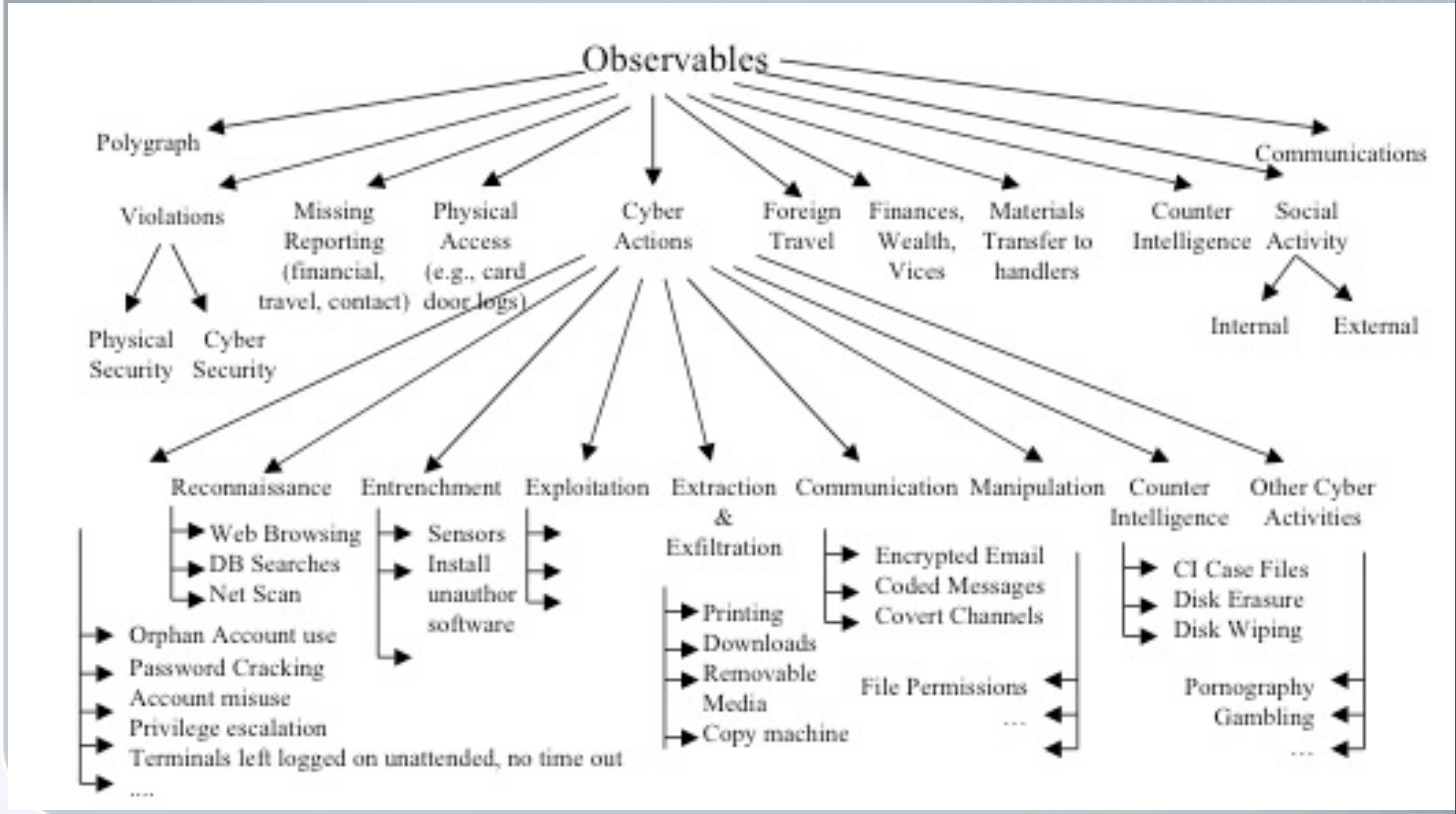
January 18, 2007 4:32 AM PST

T.J. Maxx hack exposes consumer data

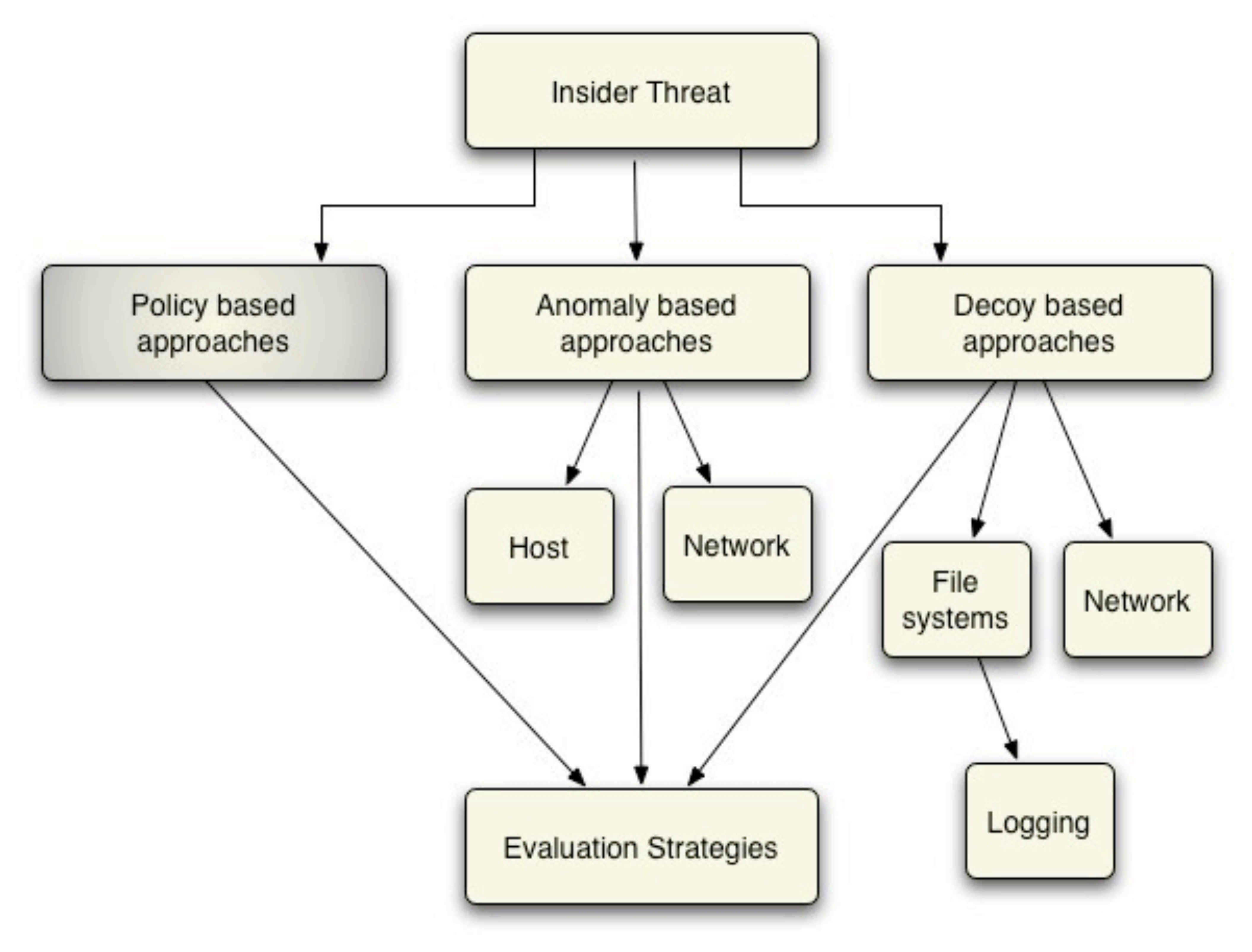
By Joris Evers
Staff Writer, CNET News

Insider Cyber Observables

- Taxonomy to characterize cyber observables [BA04]



Policy-based Prevention

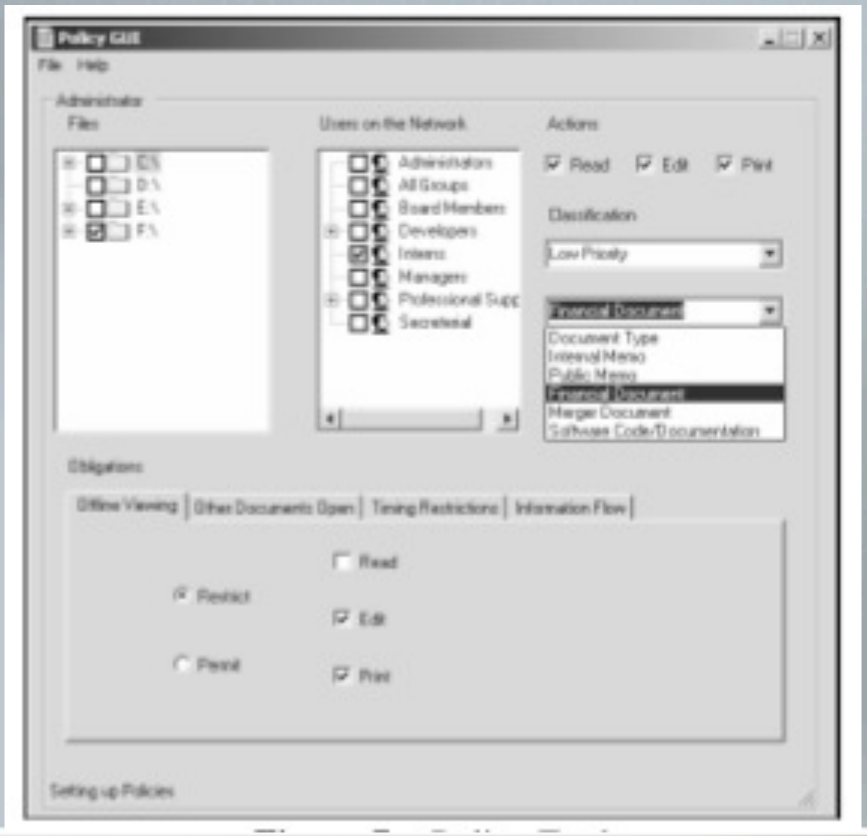


Policy-based Prevention

- Policies should specify the goals a system must meet and threats it must resist
- Many challenges for insider threat:
  - Difficult to design and maintain for organizations
  - Often have are relaxed (e.g., someone is on vacation)
  - "Explicit granting of trust creates an exception that those mechanisms honor [Bis05]"
- Traditional approaches:
  - Clark-Wilson model[CW87]: integrity
  - Bell-LaPadula model: confidentiality
- Depends on the nature of the organization (e.g. commercial vs. military)

Context aware security policies

- Policies for the document control domain with additional context [PSU04]
  - Enforces policies on “information flow”: document reading, copying, printing, forwarding, etc.
  - Looks at sequences of requests and open documents
  - Prevent illegal flow of information from one document to another.
  - Word Add-in
  - Similar to DRM?



Files
- □ C:\
- □ D:\
- □ E:\
- ☑ F:\

Users on the Network
- □ Administrators
- □ All Groups
- □ Board Members
- □ Developers
- ☑ Interns
- □ Managers
- □ Professional Supp
- □ Secretarial

Actions: ☑ Read ☑ Edit ☑ Print

Classification: Low Priority

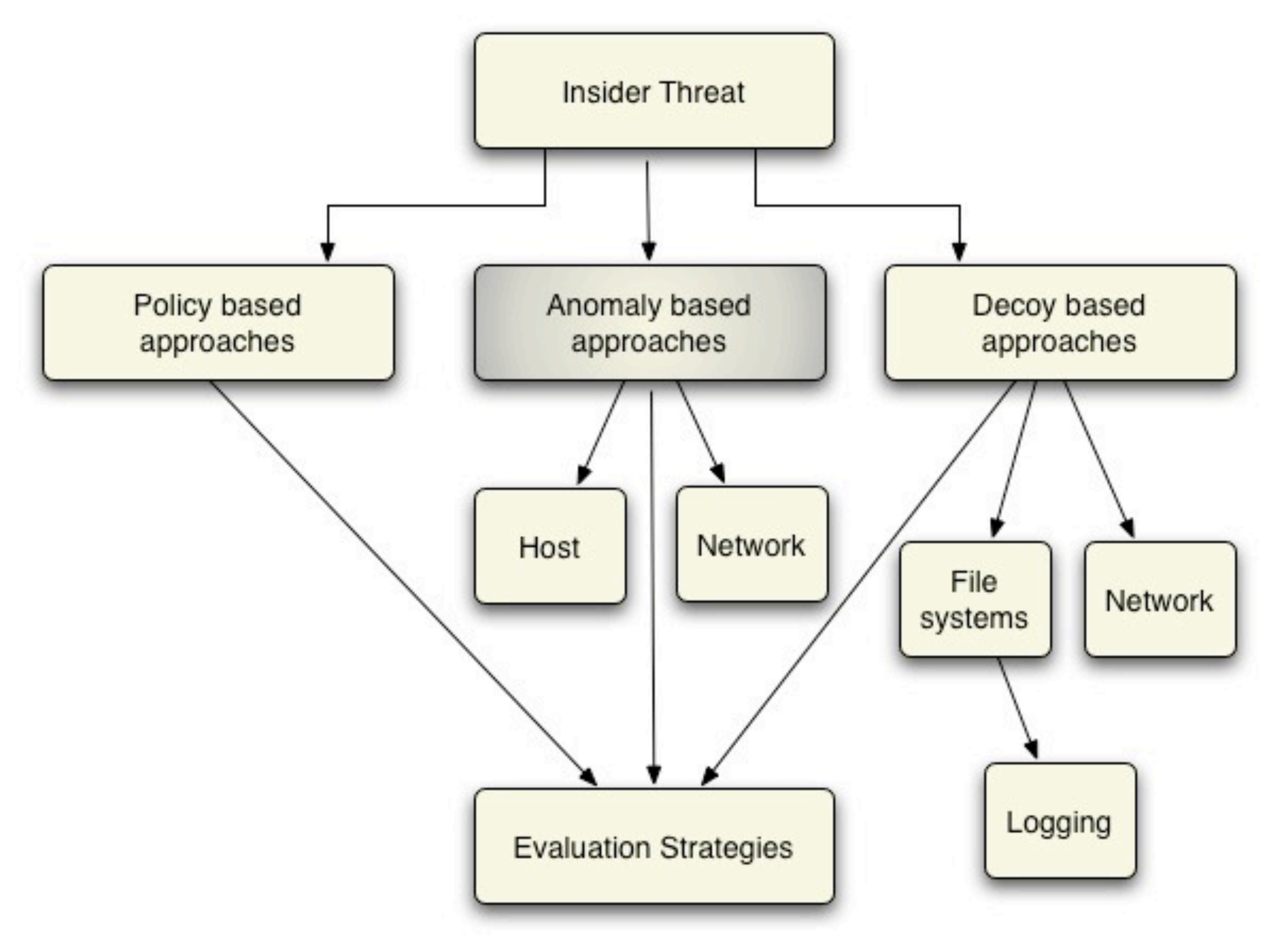
Financial Document
- Document Type
- Internal Memo
- Public Memo
- Financial Document
- Merger Document
- Software Code/Documentation

● Restrict ○ Permit

□ Read
☑ Edit
☑ Print

Setting up Policies

Anomaly Detection



Anomaly Detection

- Characterize normal insider behavior and look for deviations from it.
  - Requires that anomalous behavior can be distinguished
  - Naturally prone to varying degrees of FPs and FNs
- Many examples in this category of defense that differ in regards to:
  - Types of features
  - Number of features
  - Algorithms for building models
  - Thresholds for detection

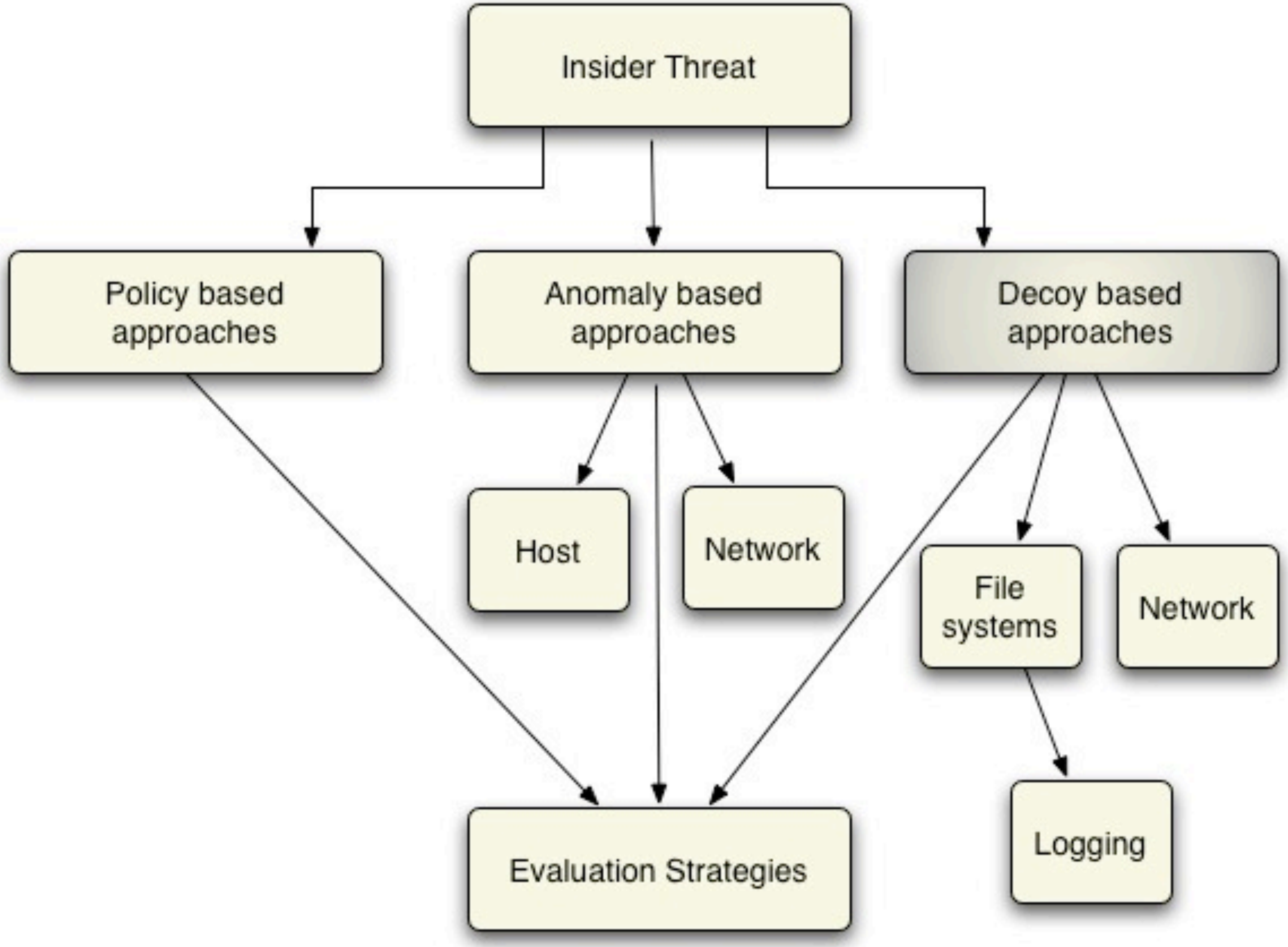
Anomaly Detection: Network

- Elicit: Leverage internal contextual information to build detectors [MS05]
  - Info from employee directory, email, projects, etc.
  - Build social networks with contextual info
  - 76 Detectors with various weights: sensitive search terms, browsing, non-local printing, etc.
  - Large dataset of 16 Tb for 3.9k users over ¾ yr
- Red team developed 15 scenarios
  - Modeled after public cases
  - Injected into dataset for evaluation
- Detection rate of .85 with FP of .015
  - Bayesian inference network for ranking

Anomaly Detection on Hosts

- Detecting insider threats by monitoring system call activity [NRK01]
  - Goal: decide if detection is possible with system calls
  - File usage patterns are too dynamic/irregular
  - Many file accesses are uninteresting (i.e., performed through automated means)
- Masquerade detection in document management system [SPU06]
  - User Word plug-in to log all user actions
  - User study with 41 people typing the same document
  - Results: avg detection rate ~58%, FP of ~14%

Decoy-based Approaches



Deception in Computer Security

- Defined: Actions to deliberately mislead hackers and cause them to take (or not take) specific actions that aid security [JDD96]
- Deception has two aspects: hiding the real and showing the false [BW82]
- Adversary's discovery process [Yuill et al 27]
  - Direct observation (recognizing)
  - Investigation (evidence collection)
  - Learning from other people or agents

Proactive detection: Decoys

- First used detailed in the "The Cuckoos Egg", by Cliff Stoll
  - Used "bait" files to catch hackers breaking into LBL
- Honeypots:
  - Deception-based information resources that have no production value other than to attract, detect, and profile adversaries
  - Honeytokens: bogus medical records, credit card numbers, and credentials [Spitzner 24]
  - Can be useful in detecting malicious insiders

Stealth Logging

- Logging is essential for profiling and detection, but must be done clandestinely
- Sebek-Kernel based data capture tool [13]:
  - De-facto standard for honeynet monitoring
  - Can detect/circumvented by attackers [DH04](e.g., memory mapped files can be read without detection)
- Recent advances:
  - Out of host monitoring for VM-based hosts [JW07]
  - Implemented as part of virtual machine monitor layer
  - Tamper-resistant and invisible to attackers

Deceptive File Systems

- Can be useful components in trap-based defense strategy

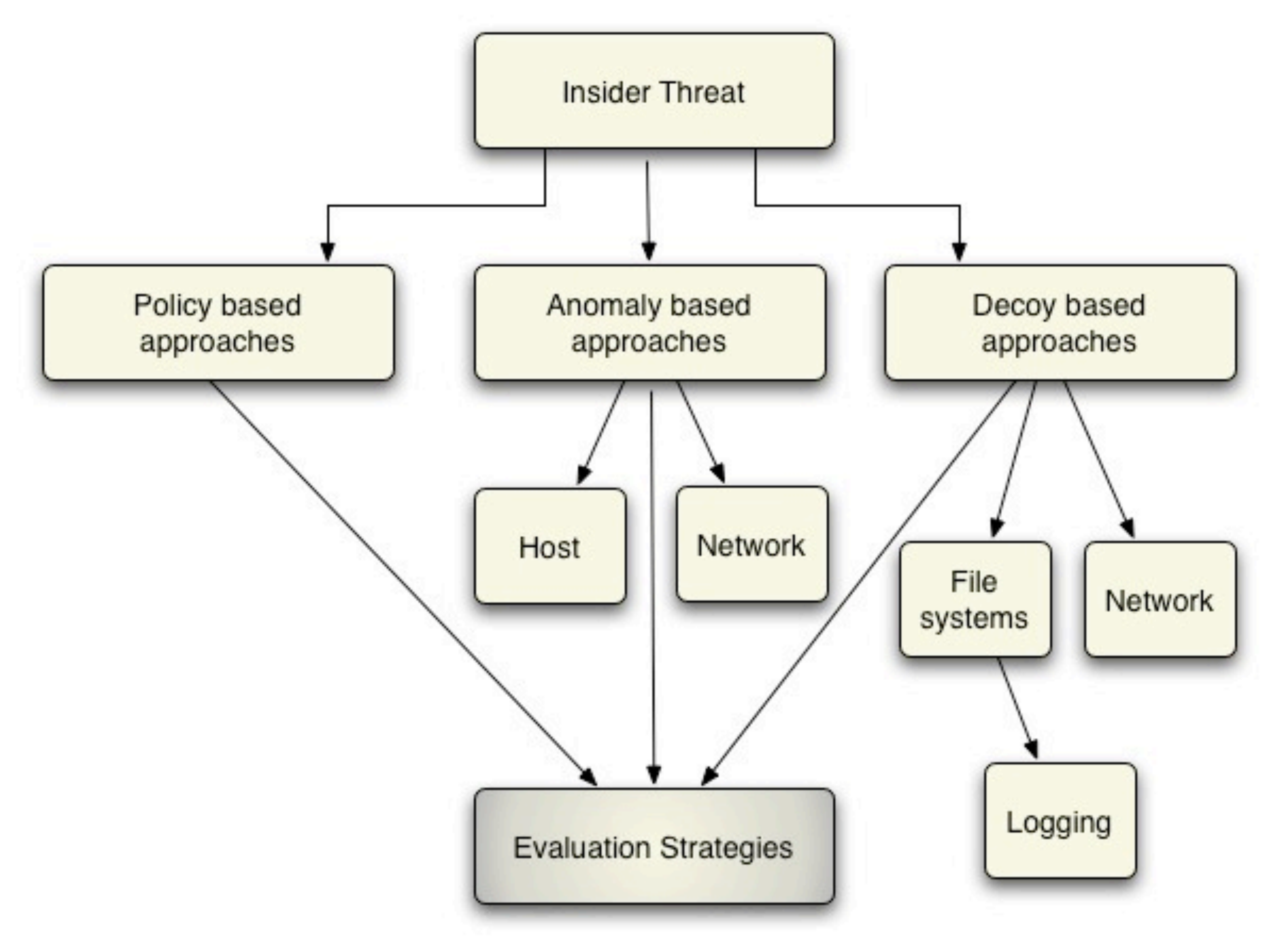
- "Honeyfiles" [YZDF04]:
  - Created a system to support the creation of bait files
  - Enhancement to the Network File Server
  - Does not focus on the content or automatic creation

- Snoopfs [ZN00]:
  - Only a files' owner or root is allowed access
  - Modified lookup routine to log alerts
  - Implemented as part of FiST, a stackable file system

Other types of network deception

- Deceptive techniques useful in other threat models may be of use to insider detection
- Web bugs :
  - Technique of email marketing companies from 90s
  - Demonstrated to be useful in detecting phishing attacks [MV07]
- Bogus network activity (Siren):
  - Fabricate network activity to detect mimicry attack [BZP06]
  - Malicious programs that mimic fake traffic are detected by collaborating IDS
  - Forces malicious software to have to pass “reverse Turing Test”

Evaluation Strategies



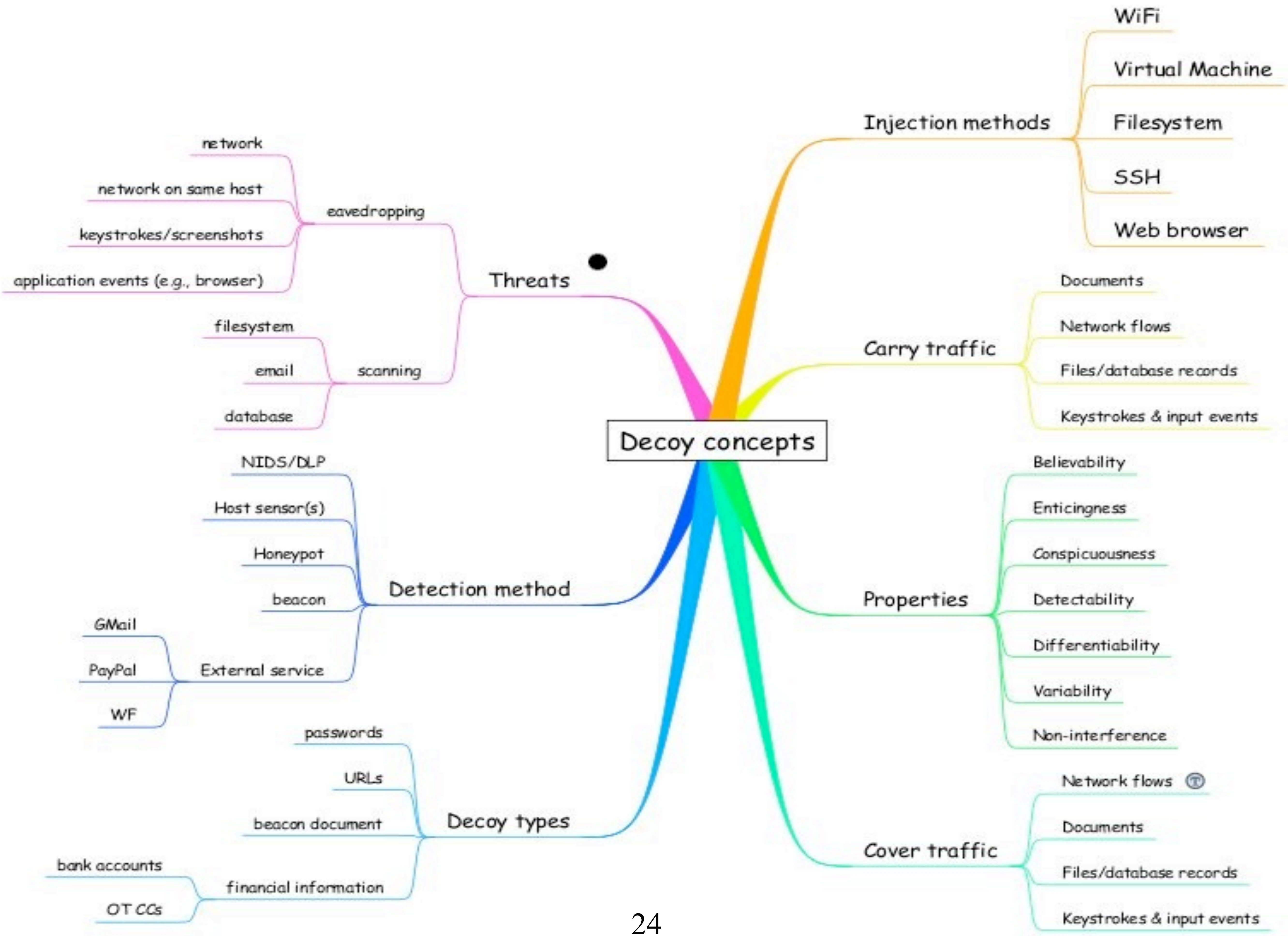
Evaluation Methodologies

- Network instrumentation of actual insider cases.
  - Elicit [May05]– Simulated 15 insiders in 3900
  - Maybury et al. [MS05] - Simulated 3 insiders in 75
- Traps against real threats
  - Bogus network: Siren [BZP06] – Detected 10 Trojans
  - Bogus credentials: Phoney [CCU06] – Detected all Phishing attacks
  - Web Bugs [MV07] – Detected 2 Phishing attacks
- Insider threat user studies
  - System call activity [NRK01] – 10 hosts, 20 users,2yrs
  - Masquerade detection [SPU06] – 41 users

Research Hypothesis

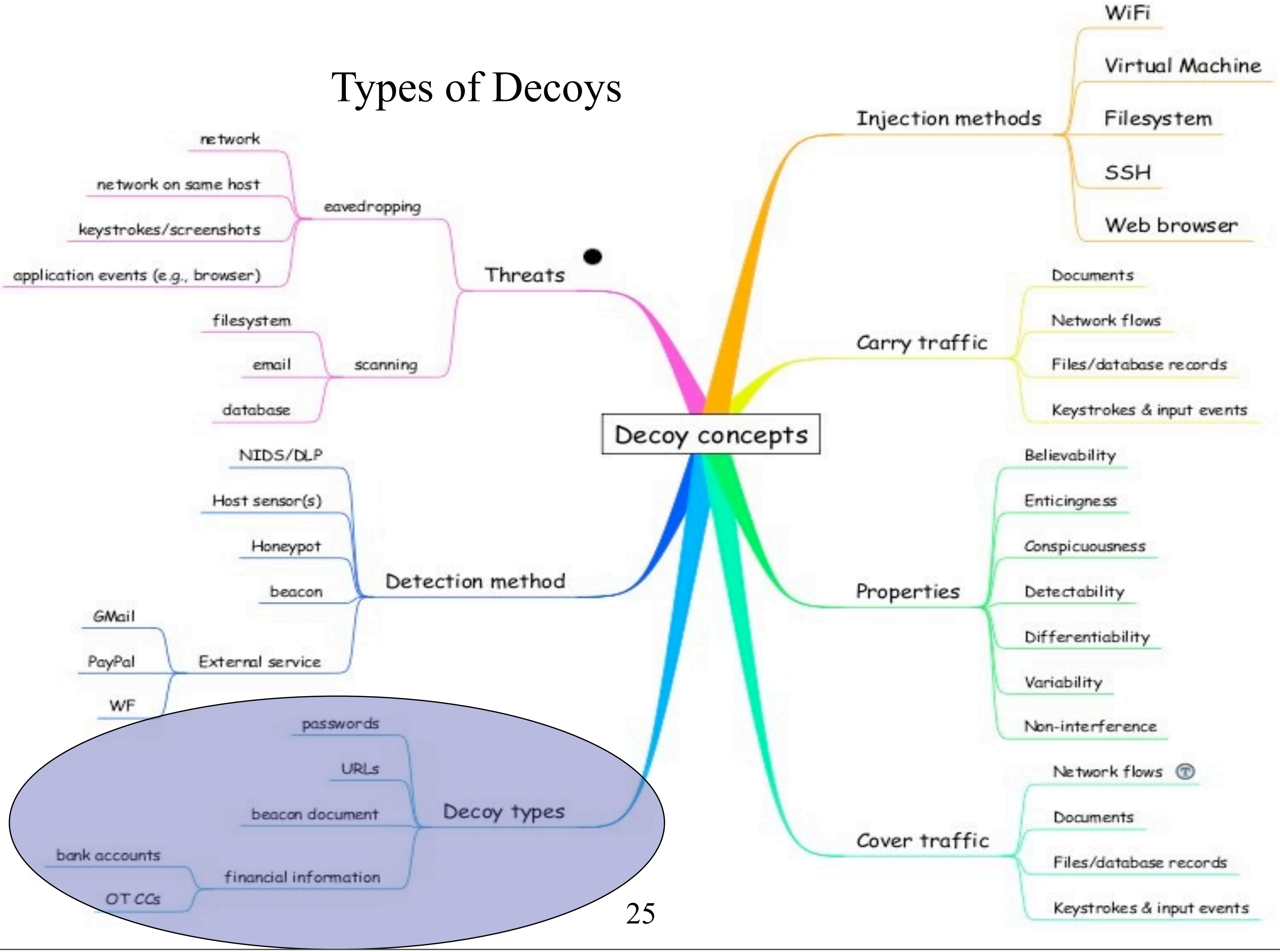
- The cyber landscape provides a vast number of settings in which decoys can be deployed.

- Hypothesis:
  - Believable decoys can be automatically generated for a variety of security problems including the detection of insider attacks, data leaks via malware and insider security violations in large organizations.



- Decoy concepts
  - Threats
    - eavedropping
      - network
      - network on same host
      - keystrokes/screenshots
      - application events (e.g., browser)
    - scanning
      - filesystem
      - email
      - database
  - Detection method
    - NIDS/DLP
    - Host sensor(s)
    - Honeypot
    - beacon
    - External service
      - GMail
      - PayPal
      - WF
  - Decoy types
    - passwords
    - URLs
    - beacon document
    - financial information
      - bank accounts
      - OT CCs
  - Injection methods
    - WiFi
    - Virtual Machine
    - Filesystem
    - SSH
    - Web browser
  - Carry traffic
    - Documents
    - Network flows
    - Files/database records
    - Keystrokes & input events
  - Properties
    - Believability
    - Enticingness
    - Conspicuousness
    - Detectability
    - Differentiability
    - Variability
    - Non-interference
  - Cover traffic
    - Network flows
    - Documents
    - Files/database records
    - Keystrokes & input events

Types of Decoys



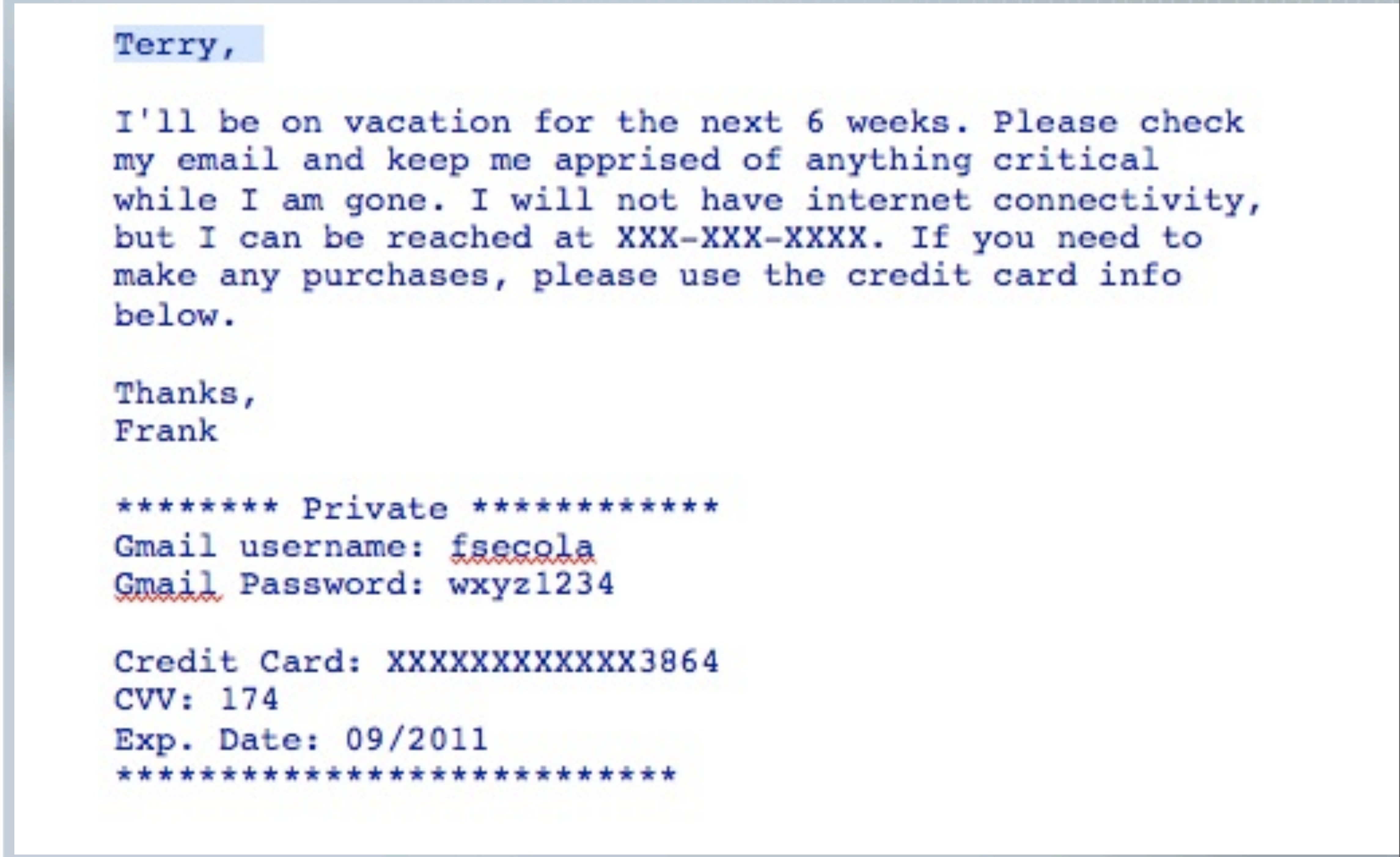
Decoy concepts

- Threats
  - eavedropping
    - network
    - network on same host
    - keystrokes/screenshots
    - application events (e.g., browser)
  - scanning
    - filesystem
    - email
    - database
- Detection method
  - NIDS/DLP
  - Host sensor(s)
  - Honeypot
  - beacon
  - External service
    - GMail
    - PayPal
    - WF
- Decoy types
  - passwords
  - URLs
  - beacon document
  - financial information
    - bank accounts
    - OT CCs
- Injection methods
  - WiFi
  - Virtual Machine
  - Filesystem
  - SSH
  - Web browser
- Carry traffic
  - Documents
  - Network flows
  - Files/database records
  - Keystrokes & input events
- Properties
  - Believability
  - Enticingness
  - Conspicuousness
  - Detectability
  - Differentiability
  - Variability
  - Non-interference
- Cover traffic
  - Network flows
  - Documents
  - Files/database records
  - Keystrokes & input events

Types of Decoys

- Documents with embedded beacons (PDF and Word documents)
  - Tax documents, receipts, bank statements
- Credentials
  - Gmail, university accounts, etc
  - Example: university credentials created that appear to be from real students.
- Financial information
  - PayPal accounts
  - Collaborative effort with a financial institute

Example Theme: Delegation



Terry,

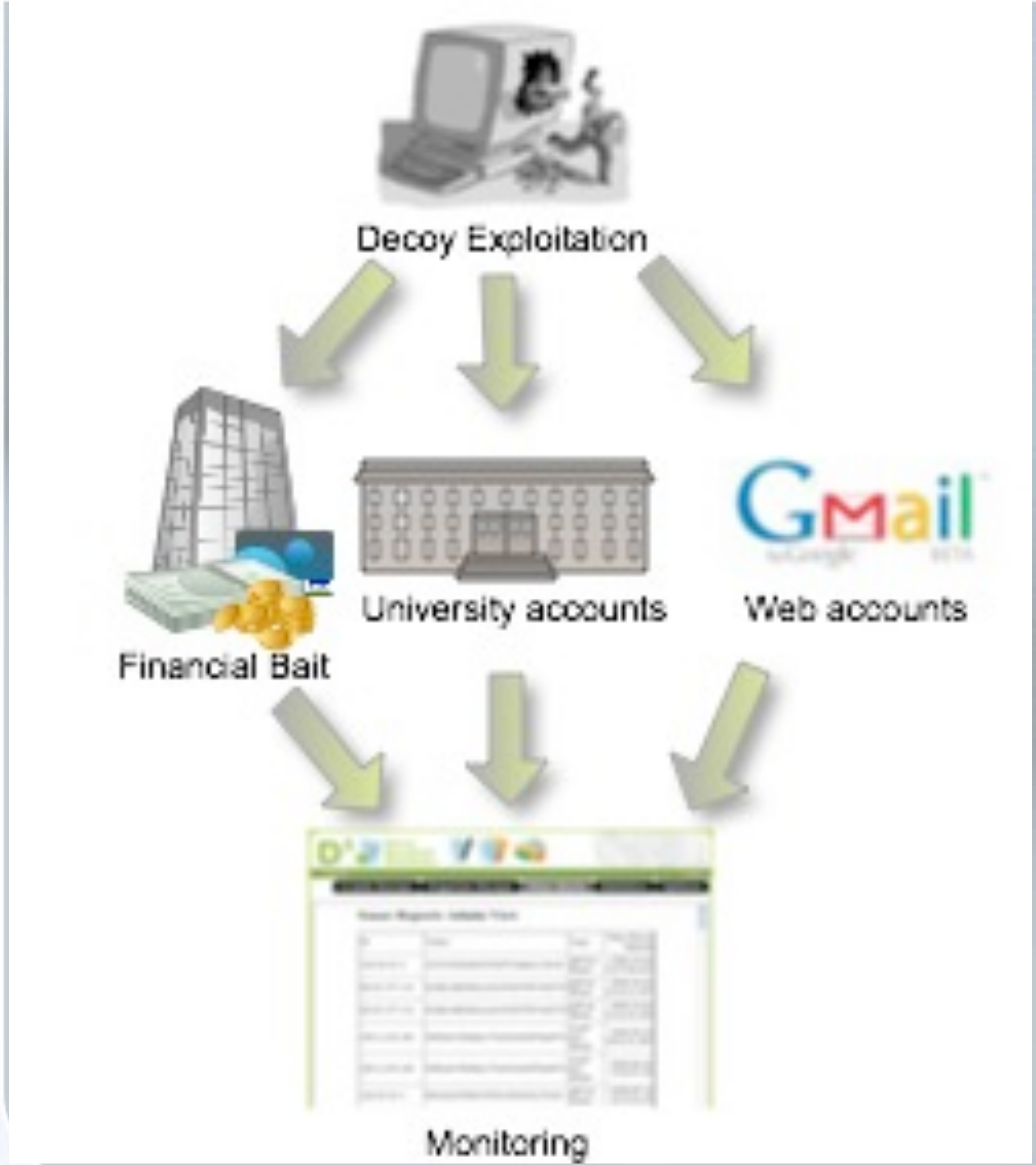
I'll be on vacation for the next 6 weeks. Please check my email and keep me apprised of anything critical while I am gone. I will not have internet connectivity, but I can be reached at XXX-XXX-XXXX. If you need to make any purchases, please use the credit card info below.

Thanks,
Frank

```
******** Private ************
Gmail username: fsecola
Gmail Password: wxyz1234

Credit Card: XXXXXXXXXXXX3864
CVV: 174
Exp. Date: 09/2011
***************************
```

Monitoring of Decoys



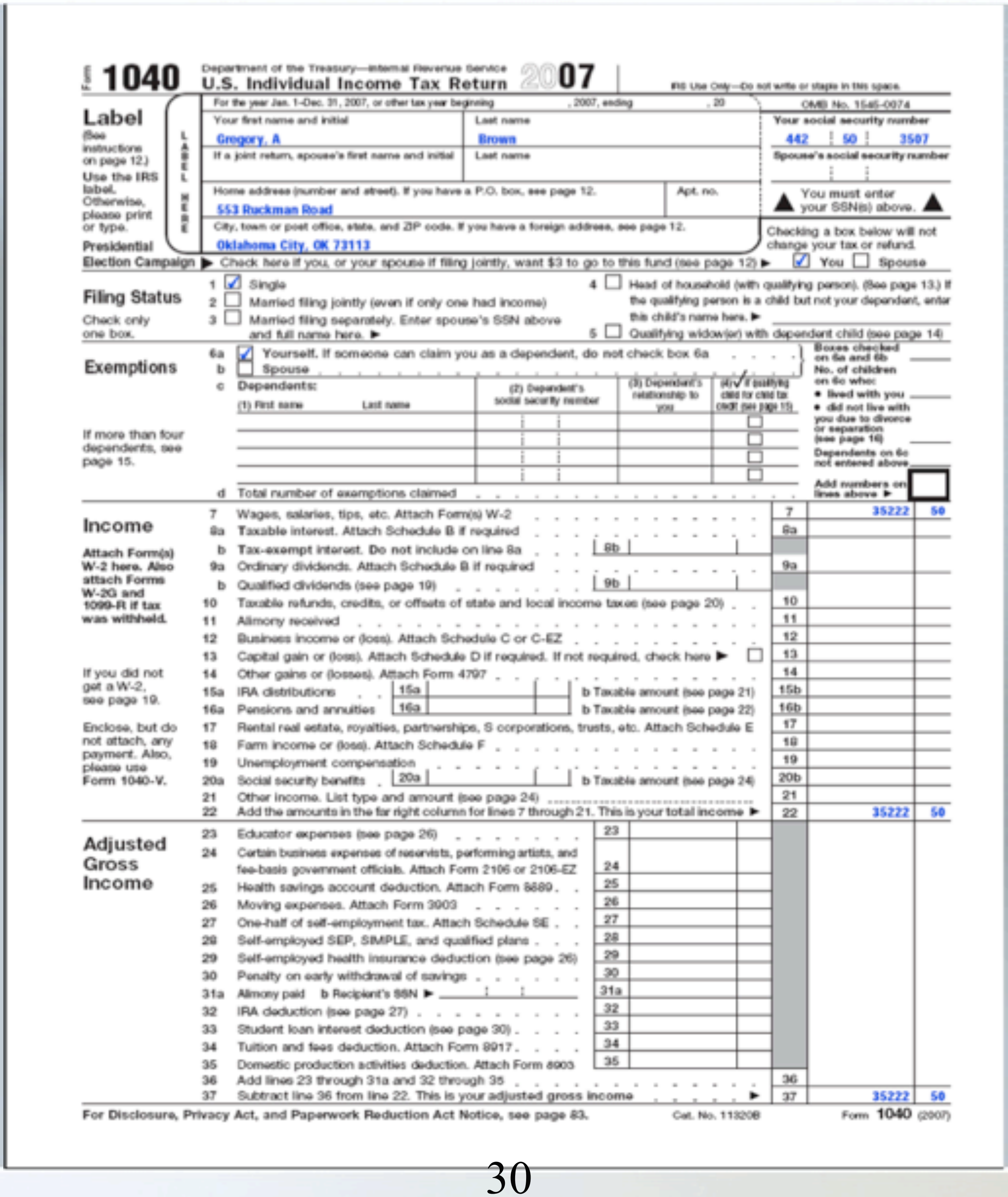
Decoy Document Distributor (D^3)

- Supports a trap-based defense to detect when insiders attempt to exfiltrate

- Novel service of automating the creation and management of decoys

- Design of decoys combines a number of methods and monitors
  - Documents with decoy credentials
  - Beacon documents
  - Signatures identifiable by a NIDs

Sample Beacon Document



Form **1040** Department of the Treasury—Internal Revenue Service
U.S. Individual Income Tax Return 2007
IRS Use Only—Do not write or staple in this space.

Label (See instructions on page 12.) Use the IRS label. Otherwise, please print or type.

LABEL HERE

For the year Jan. 1–Dec. 31, 2007, or other tax year beginning , 2007, ending , 20 OMB No. 1545-0074

Your first name and initial: Gregory, A
Last name: Brown
Your social security number: 442 50 3507

If a joint return, spouse's first name and initial
Last name
Spouse's social security number

Home address (number and street). If you have a P.O. box, see page 12.: 553 Ruckman Road
Apt. no.

▲ You must enter your SSN(s) above. ▲

City, town or post office, state, and ZIP code. If you have a foreign address, see page 12.: Oklahoma City, OK 73113

Checking a box below will not change your tax or refund.

Presidential Election Campaign ▶ Check here if you, or your spouse if filing jointly, want $3 to go to this fund (see page 12) ▶ ☑ You □ Spouse

Filing Status
Check only one box.

1 ☑ Single
2 □ Married filing jointly (even if only one had income)
3 □ Married filing separately. Enter spouse's SSN above and full name here. ▶
4 □ Head of household (with qualifying person). (See page 13.) If the qualifying person is a child but not your dependent, enter this child's name here. ▶
5 □ Qualifying widow(er) with dependent child (see page 14)

Exemptions

6a ☑ Yourself. If someone can claim you as a dependent, do not check box 6a
b □ Spouse
c Dependents:

(1) First name	Last name	(2) Dependent's social security number	(3) Dependent's relationship to you	(4) ✓ if qualifying child for child tax credit (see page 15)
				□
				□
				□
				□

If more than four dependents, see page 15.

d Total number of exemptions claimed

Boxes checked on 6a and 6b
No. of children on 6c who:
- lived with you
- did not live with you due to divorce or separation (see page 16)

Dependents on 6c not entered above
Add numbers on lines above ▶

Income

Attach Form(s) W-2 here. Also attach Forms W-2G and 1099-R if tax was withheld.

If you did not get a W-2, see page 19.

Enclose, but do not attach, any payment. Also, please use Form 1040-V.

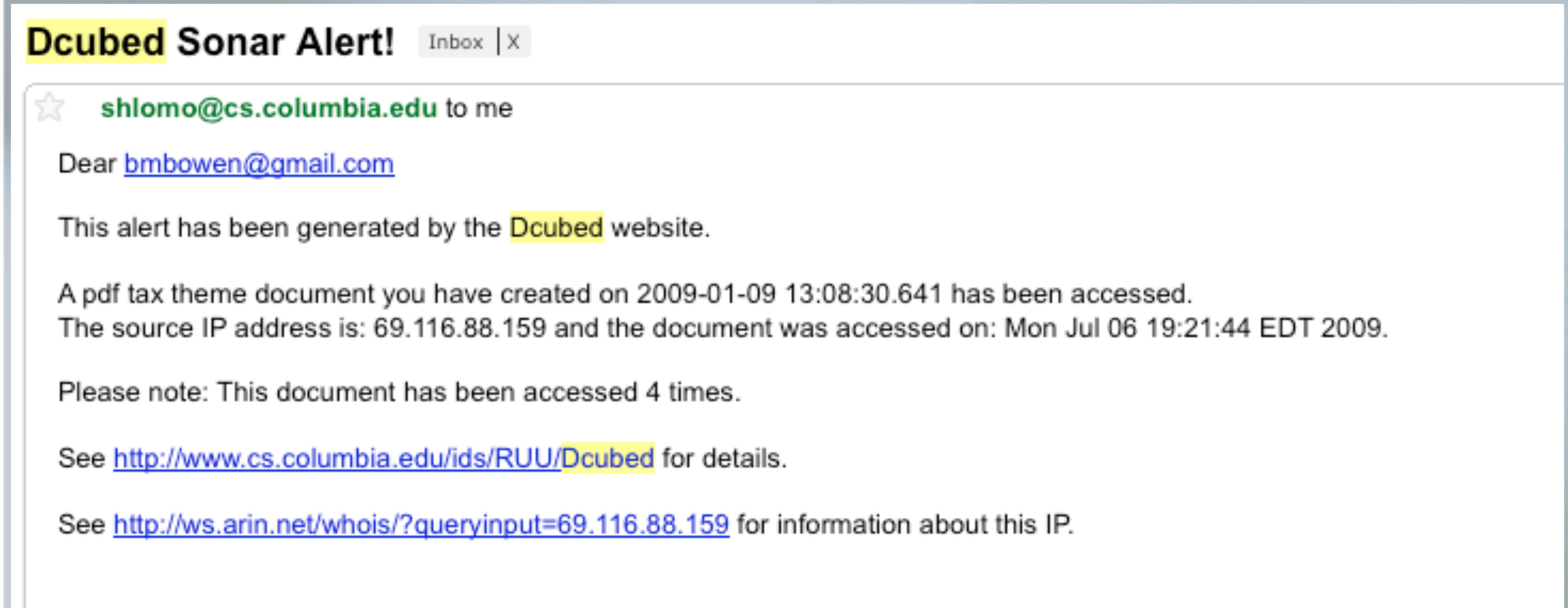
7	Wages, salaries, tips, etc. Attach Form(s) W-2			7	35222	50
8a	Taxable interest. Attach Schedule B if required			8a		
b	Tax-exempt interest. Do not include on line 8a	8b				
9a	Ordinary dividends. Attach Schedule B if required			9a		
b	Qualified dividends (see page 19)	9b				
10	Taxable refunds, credits, or offsets of state and local income taxes (see page 20)			10		
11	Alimony received			11		
12	Business income or (loss). Attach Schedule C or C-EZ			12		
13	Capital gain or (loss). Attach Schedule D if required. If not required, check here ▶ □			13		
14	Other gains or (losses). Attach Form 4797			14		
15a	IRA distributions	15a		15b		
	b Taxable amount (see page 21)					
16a	Pensions and annuities	16a		16b		
	b Taxable amount (see page 22)					
17	Rental real estate, royalties, partnerships, S corporations, trusts, etc. Attach Schedule E			17		
18	Farm income or (loss). Attach Schedule F			18		
19	Unemployment compensation			19		
20a	Social security benefits	20a		20b		
	b Taxable amount (see page 24)					
21	Other income. List type and amount (see page 24)			21		
22	Add the amounts in the far right column for lines 7 through 21. This is your total income ▶			22	35222	50

Adjusted Gross Income

23	Educator expenses (see page 26)	23				
24	Certain business expenses of reservists, performing artists, and fee-basis government officials. Attach Form 2106 or 2106-EZ	24				
25	Health savings account deduction. Attach Form 8889	25				
26	Moving expenses. Attach Form 3903	26				
27	One-half of self-employment tax. Attach Schedule SE	27				
28	Self-employed SEP, SIMPLE, and qualified plans	28				
29	Self-employed health insurance deduction (see page 26)	29				
30	Penalty on early withdrawal of savings	30				
31a	Alimony paid b Recipient's SSN ▶	31a				
32	IRA deduction (see page 27)	32				
33	Student loan interest deduction (see page 30)	33				
34	Tuition and fees deduction. Attach Form 8917	34				
35	Domestic production activities deduction. Attach Form 8903	35				
36	Add lines 23 through 31a and 32 through 35			36		
37	Subtract line 36 from line 22. This is your adjusted gross income ▶			37	35222	50

For Disclosure, Privacy Act, and Paperwork Reduction Act Notice, see page 83. Cat. No. 11320B Form **1040** (2007)

Sample Alert



Dcubed Sonar Alert!

shlomo@cs.columbia.edu to me

Dear bmbowen@gmail.com

This alert has been generated by the Dcubed website.

A pdf tax theme document you have created on 2009-01-09 13:08:30.641 has been accessed.
The source IP address is: 69.116.88.159 and the document was accessed on: Mon Jul 06 19:21:44 EDT 2009.

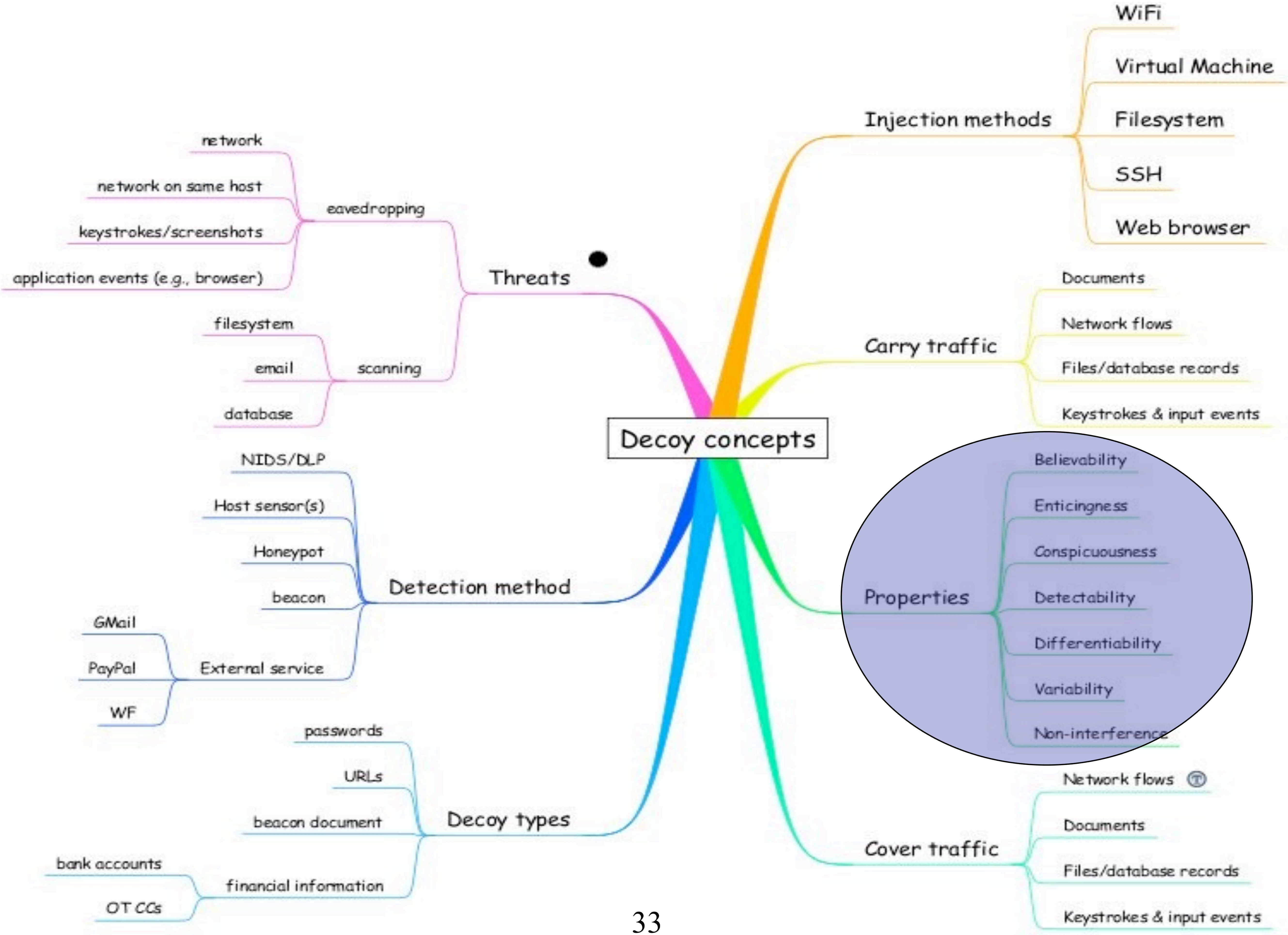
Please note: This document has been accessed 4 times.

See http://www.cs.columbia.edu/ids/RUU/Dcubed for details.

See http://ws.arin.net/whois/?queryinput=69.116.88.159 for information about this IP.

Level of Attacker Sophistication

- Low: Direct observation is the only tool. Does it pass the first glance test?
- Medium: capable of a more thorough investigation; outside information can be used
- High: use of highly sophisticated tools
- Highly Privileged: Aware that system is baited; most difficult to defend against



- Decoy concepts
  - Injection methods
    - WiFi
    - Virtual Machine
    - Filesystem
    - SSH
    - Web browser
  - Carry traffic
    - Documents
    - Network flows
    - Files/database records
    - Keystrokes & input events
  - Properties
    - Believability
    - Enticingness
    - Conspicuousness
    - Detectability
    - Differentiability
    - Variability
    - Non-interference
  - Cover traffic
    - Network flows ⓣ
    - Documents
    - Files/database records
    - Keystrokes & input events
  - Threats ●
    - eavedropping
      - network
      - network on same host
      - keystrokes/screenshots
      - application events (e.g., browser)
    - scanning
      - filesystem
      - email
      - database
  - Detection method
    - NIDS/DLP
    - Host sensor(s)
    - Honeypot
    - beacon
    - External service
      - GMail
      - PayPal
      - WF
  - Decoy types
    - passwords
    - URLs
    - beacon document
    - financial information
      - bank accounts
      - OT CCs

Decoy Properties

- Novel set of generally applicable decoy properties
- Guide the design and deployment of decoys
- Aid in maximizing the deception that decoys in induce

Believable: appearing to be true

- Goal: Make it difficult for an adversary to discern what is fake from what is real
- Perfect decoy: completely indistinguishable from authentic
- Possibly unachievable, but provides a goal to strive toward
- For many threats, it might suffice to have a less than perfect decoy

Believability Formalization

- Defined for document space M and decoy set D
- Decoy Believability Experiment
  - For any d $\in$ D, choose two documents m_0 ,$m_1 \in$ M such that m_0 =d or m_1=d, and $m_0 \neq m_1$
  - Adversary A obtains m_0, m_1 and attempts to choose m' $\in \{m_0, m_1\}$ such that m' != d, using only information intrinsic to m_0, m_1
  - The output of the experiment is 1 if m' != d and 0 otherwise.
- Perfect decoy when: $\Pr[\mathrm{Exp}_{\mathrm{believe}} = 1] = 1/2$

Detectable: exhibit an observable artifact

- Emit a beacon when opened
  - Limited to certain applications
- Alert when decoy credentials are exploited
- $\Pr[d \to M : \text{Alert } A,d = 1] \geq \varepsilon$

Enticing: highly Attractive

- How to measure the amount of lure?
- Perhaps monetary value (credit cards and credentials have value on the black market)
  - Credit card number $1.20
  - PayPal accounts $3-50 depending on balance
- Depends on attacker intent
  - Posit: by defining categories of "attacker interest", one may construct decoys of containing terms of attacker interest.

Enticing Formalization

- For document space M, let P be the set of documents of an adversary's preference, where $P \subseteq M$

- For $\varepsilon > 1/|M|$ we define an enticing document with the probability:

  $\Pr[m \rightarrow M | m \in P] > \varepsilon$

- An enticing decoy is then defined for the set of decoys D, where $D \subseteq M$, such that:

  $\Pr[m \rightarrow M | m \in P] = \Pr[d \rightarrow M | d \in D]$

Variability: over possible outcomes

- Decoys should not be identifiable due to some invariant or signature

- A good decoy generator should produce an unbounded collection of variable decoys with respect to string content

- Perfecly variable:$\Pr[d_{,} \rightarrow D : \mathrm{Exp}_{\mathrm{believe}_{,}} = 1] = 1/2$

- N-strong Variant: determine the N+1st decoy only after observing the N prior

Conspicuous: easily visible

- Decoys should be easily found or observed to be of value
  - For example "password.txt"
- Can be measured by the number of user actions taken before one encounters a decoy
- If a decoy is never encountered, its not conspicuous

Non-interference: doesn't hinder

- Decoys should not interfere with normal user operations
- The more believable a decoy, the more likely a legitimate user will be ensnared
- Implies another property to *differentiate* bogus information from the authentic
- Defining formally in terms of success

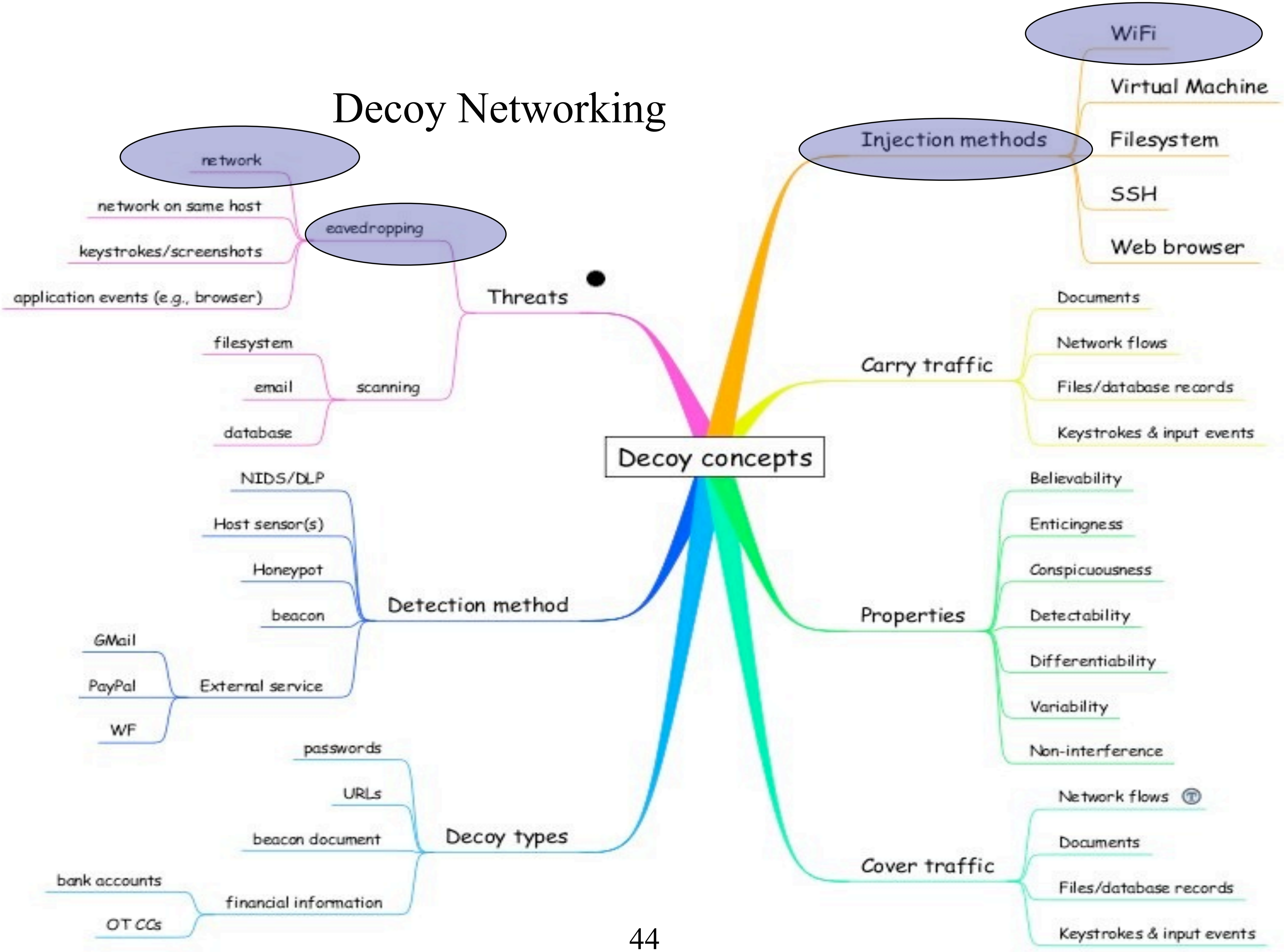
Differentiable: by the user

- Important that decoys be "obvious" to the legitimate user

- Important to be "unobvious" to the insider stealing information.

- $\Pr[\mathrm{Exp}_{\mathrm{believe}} = 1] = 1$

Decoy Networking



- Decoy concepts
  - Threats
    - eavedropping
      - network
      - network on same host
      - keystrokes/screenshots
      - application events (e.g., browser)
    - scanning
      - filesystem
      - email
      - database
  - Detection method
    - NIDS/DLP
    - Host sensor(s)
    - Honeypot
    - beacon
    - External service
      - GMail
      - PayPal
      - WF
  - Decoy types
    - passwords
    - URLs
    - beacon document
    - financial information
      - bank accounts
      - OT CCs
  - Injection methods
    - WiFi
    - Virtual Machine
    - Filesystem
    - SSH
    - Web browser
  - Carry traffic
    - Documents
    - Network flows
    - Files/database records
    - Keystrokes & input events
  - Properties
    - Believability
    - Enticingness
    - Conspicuousness
    - Detectability
    - Differentiability
    - Variability
    - Non-interference
  - Cover traffic
    - Network flows
    - Documents
    - Files/database records
    - Keystrokes & input events

Decoy Networking: Snoopers

- In general, there is little that can be done to detect passive eavesdropping on networks.
- Some general techniques for detecting snoopers are based on DNS behavior or network and machine latency.
- Problem is exacerbated with WiFi due to range of signals and the absence of physical barriers

Decoy Networking: Threat model

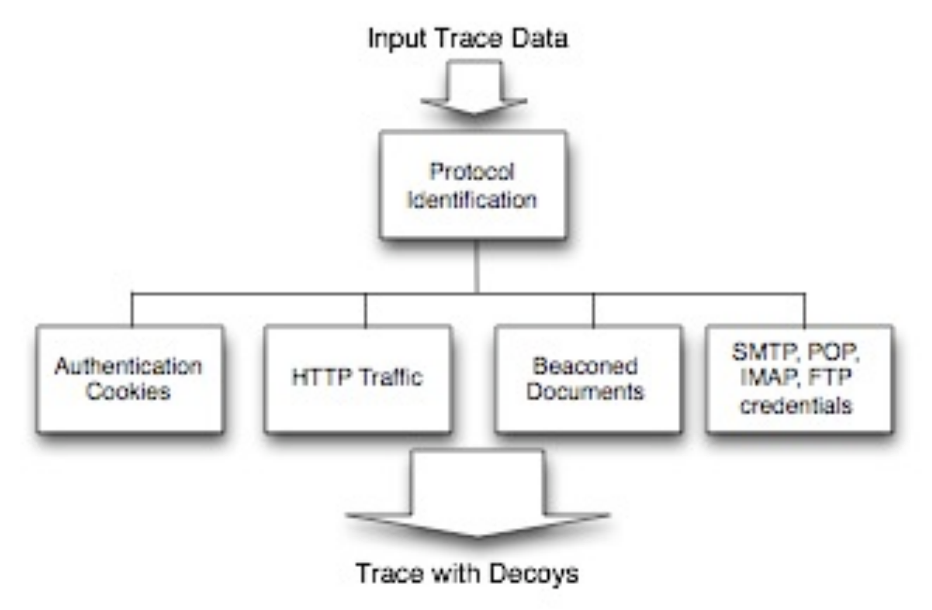
- Methodology is demonstrated for WiFi, but can be applied to wired networks
- Insiders, who legitimately have access to a network, but attempt to use it for attaining illegitimate goals.
- External attacks at protocol level via password guessing, router hijacking, or some vulnerability in WiFi security.
  - Only 49% of corporate access points in NYC and 48% in London used advanced security [Cracknell08]

Decoy Networking: Approach

- Injection decoy traffic with bait information to force attacker into observable action
- Target semantic information sought by attackers rather than network-level observables like previous work
- Aim to maximize the realism of decoy traffic with a novel architecture based on a “record, modify, replay” paradigm

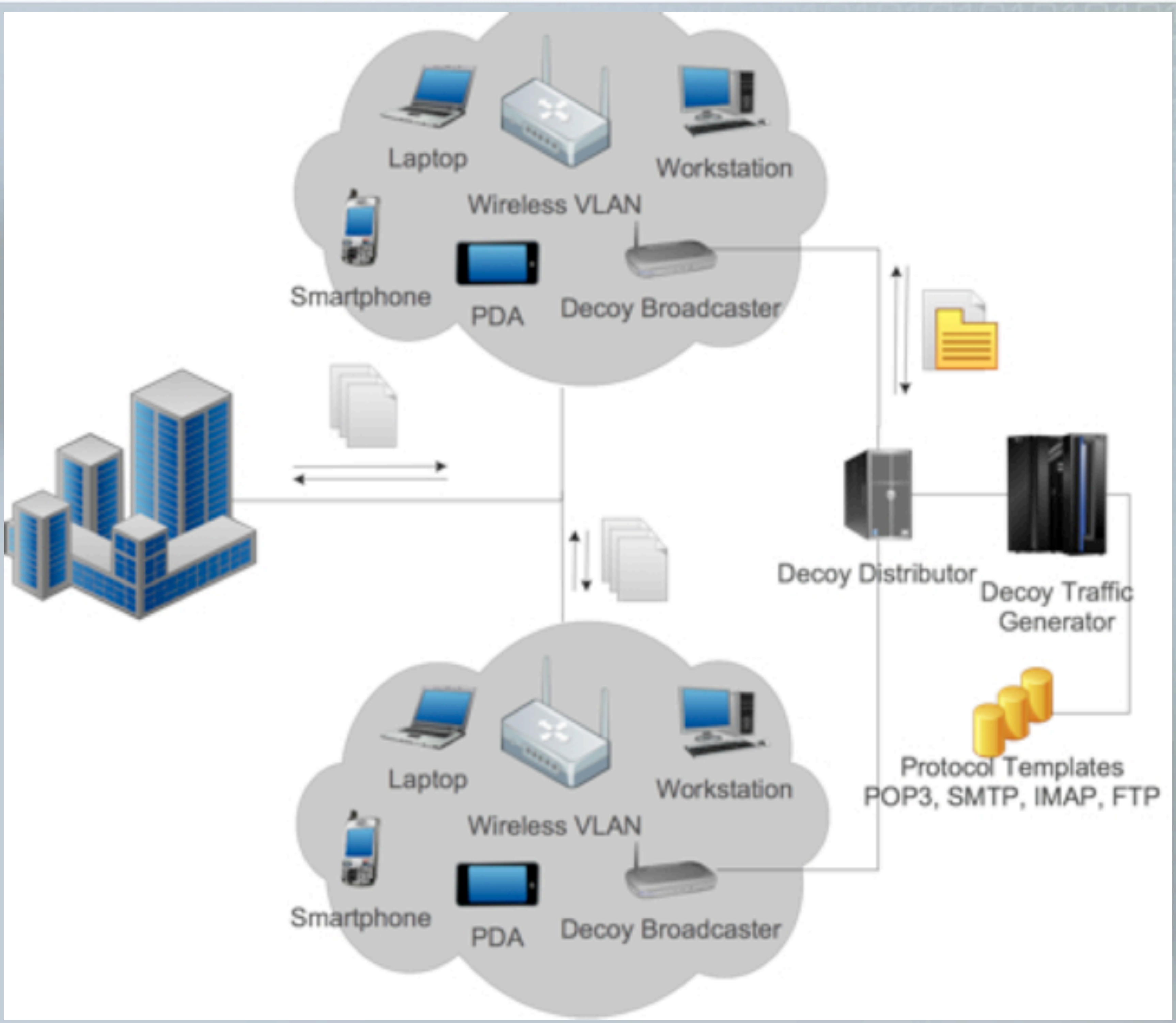
Architecture

- Decoy Traffic Generator
  - Templates for input



- Decoy Broadcaster
  - Inexpensive mechanism for broadcasting bait content over a network
  - Placed in the vicinity of a legitimate access point so as to maximize the coverage of the replayed traffic

Architecture



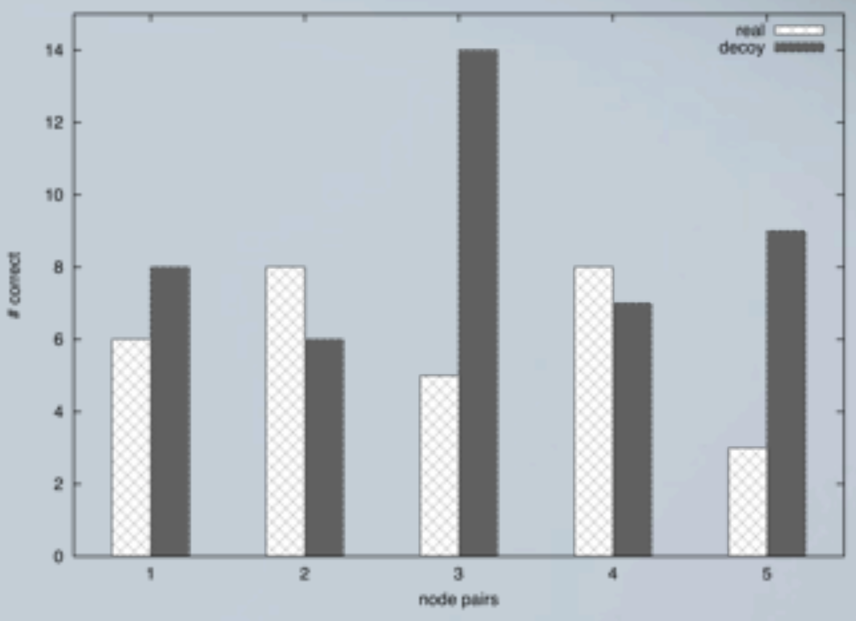
Believability: A Decoy Turing Test

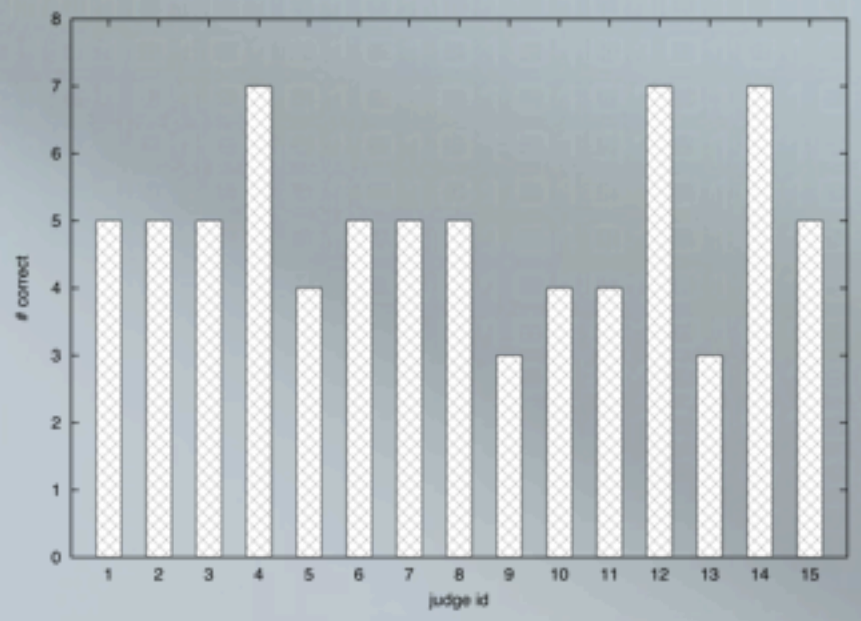
- Rely on human judges to distinguish authentic and machine generated decoy network traffic

- Experiment Summary:
  - Judges included PhD's and graduate students in the network security field, CRF, and an antivirus company
  - Recording traffic from 5 hosts on a private network using test identities
  - Trace was passed to the honeyflow creation to produce honeyflows for each of the 5 hosts.
  - Resulting test data set included traffic from 10 hosts

Decoy Turing Test Results

- Overall, the judges were 49.9% correct, on average, suggesting that we have achieved the goal of indistinguishable decoys

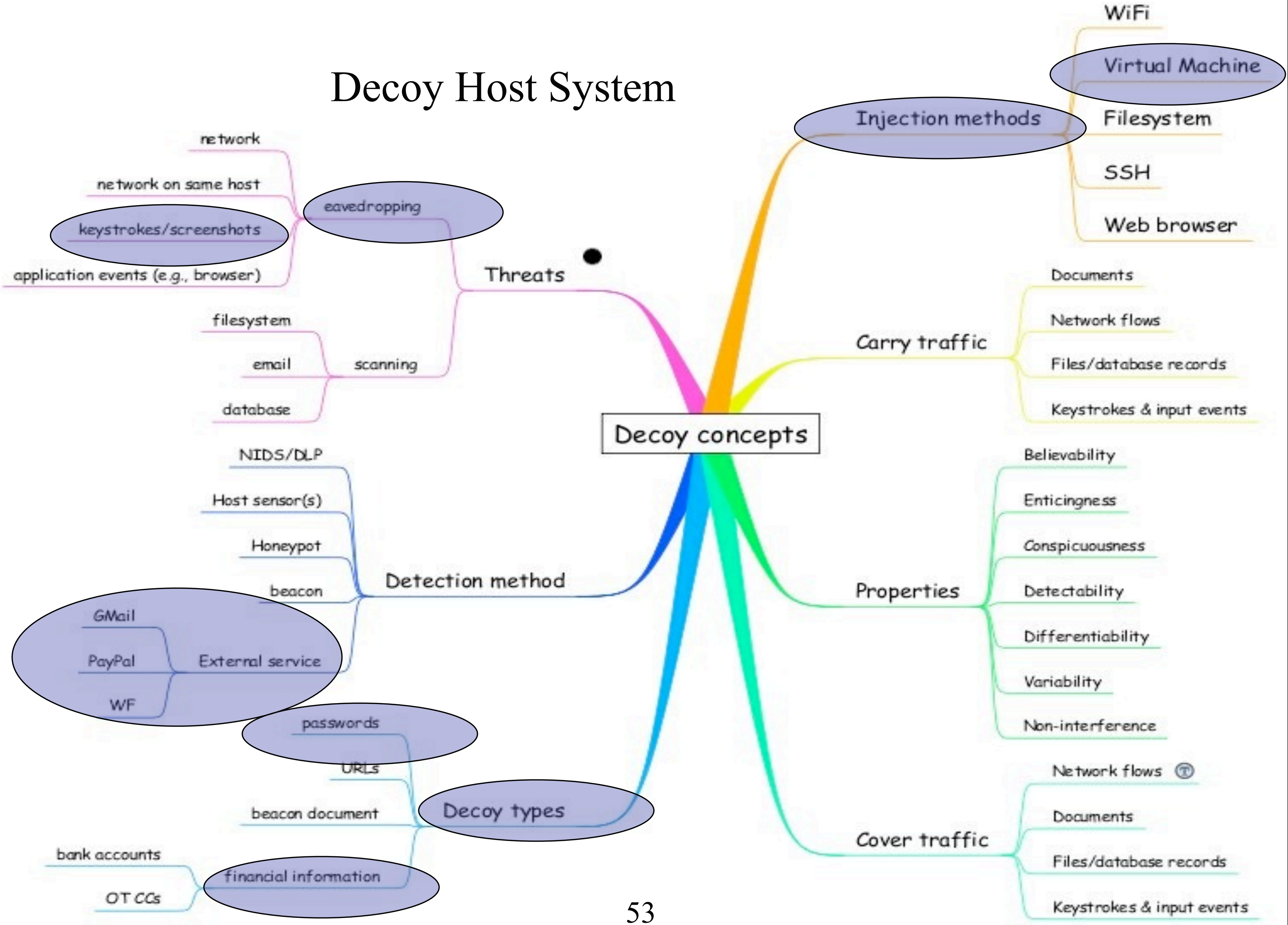




Experiments in the Field

- Defcon
  - Gmail decoy alert was triggered after someone logged into one of our Gmail accounts from an IP address in New Jersey, shortly after the account was used in Las Vegas.
  - We believe the decoy was the victim of a cookie hijacking attack
- Massive Cookie Harvesting
  - Developed model attack program is called Gsnoop to sniff and record Gmail login cookies
  - Gsnoop uses the cookie to log into the account
  - Results: one alert for each of the decoys

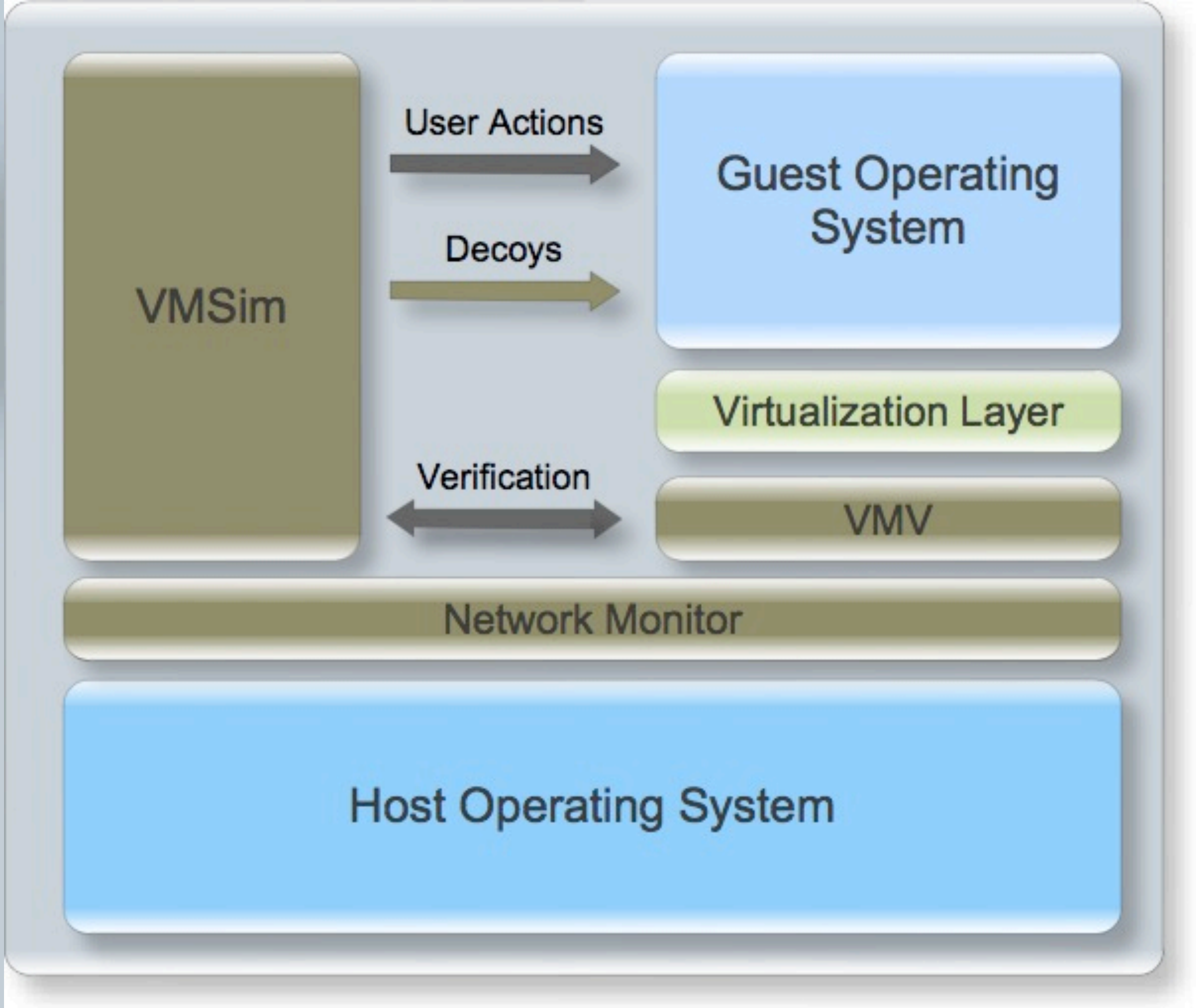
Decoy Host System



Decoy Host System

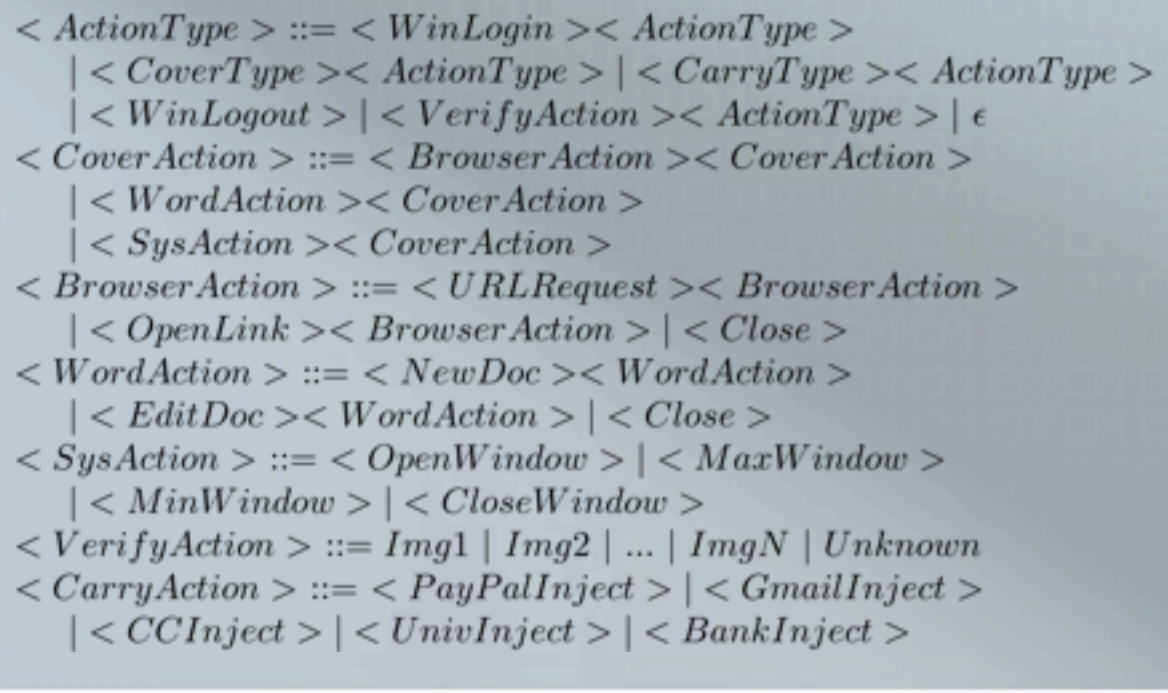
- Threat Model
  - Attacker lacks long-term physical access, but has the capability to install malicious software
  - May be used for long term reconnaissance or to steal information of value
- BotSwindler:
  - Designed to be tamper resistant by malware
  - For injection Believable Decoys in VM-Based Hosts for malware Detection
- Demonstrate the believability and detection of malware with financial bait

BotSwindler Components



VMSim

- General goals
  - Simulator process remains undetected by the malware
  - The actions of the simulator appear to be generated by a human.
- Simulates X11 mouse and keyboard events from outside the host
- Formal Language:



$$
\begin{aligned}
&< ActionType > ::= < WinLogin >< ActionType > \\
&\quad | < CoverType >< ActionType > | < CarryType >< ActionType > \\
&\quad | < WinLogout > | < VerifyAction >< ActionType > | \epsilon \\
&< CoverAction > ::= < BrowserAction >< CoverAction > \\
&\quad | < WordAction >< CoverAction > \\
&\quad | < SysAction >< CoverAction > \\
&< BrowserAction > ::= < URLRequest >< BrowserAction > \\
&\quad | < OpenLink >< BrowserAction > | < Close > \\
&< WordAction > ::= < NewDoc >< WordAction > \\
&\quad | < EditDoc >< WordAction > | < Close > \\
&< SysAction > ::= < OpenWindow > | < MaxWindow > \\
&\quad | < MinWindow > | < CloseWindow > \\
&< VerifyAction > ::= Img1 \mid Img2 \mid ... \mid ImgN \mid Unknown \\
&< CarryAction > ::= < PayPalInject > | < GmailInject > \\
&\quad | < CCInject > | < UnivInject > | < BankInject >
\end{aligned}
$$

Virtual Machine Verification

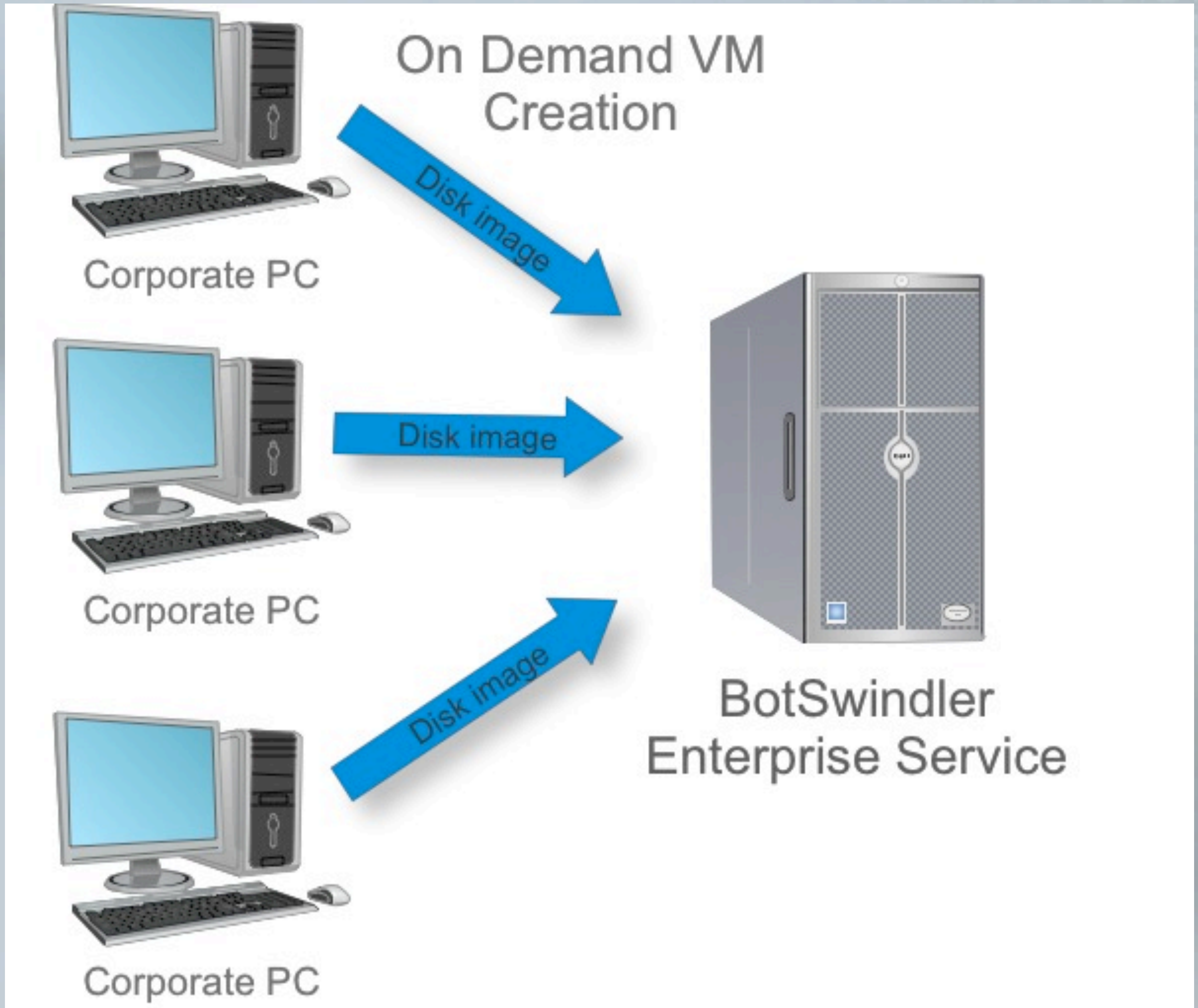
- Simulator challenge lies in generating human-like events in the face of variable host responses (due to network latency, OS issues, and changes to web content)

- Approach: decide whether the current VM state is in one of a predefined set of states.

- States are defined with graphical artifacts or pixel selections

- State monitoring is built into the VMM

Application in an enterprise

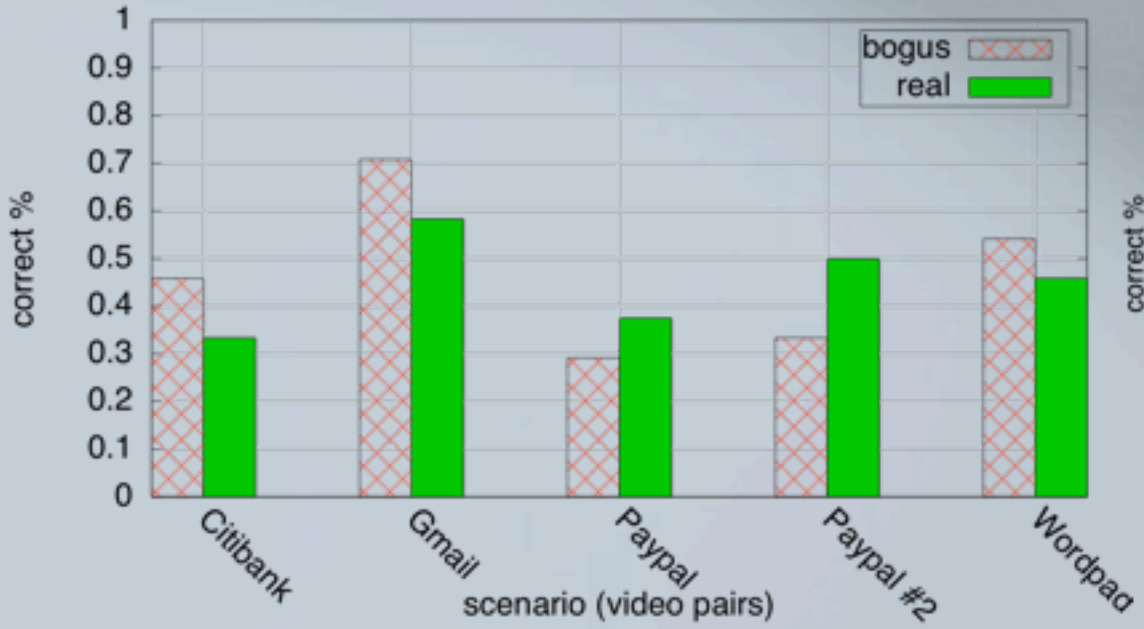


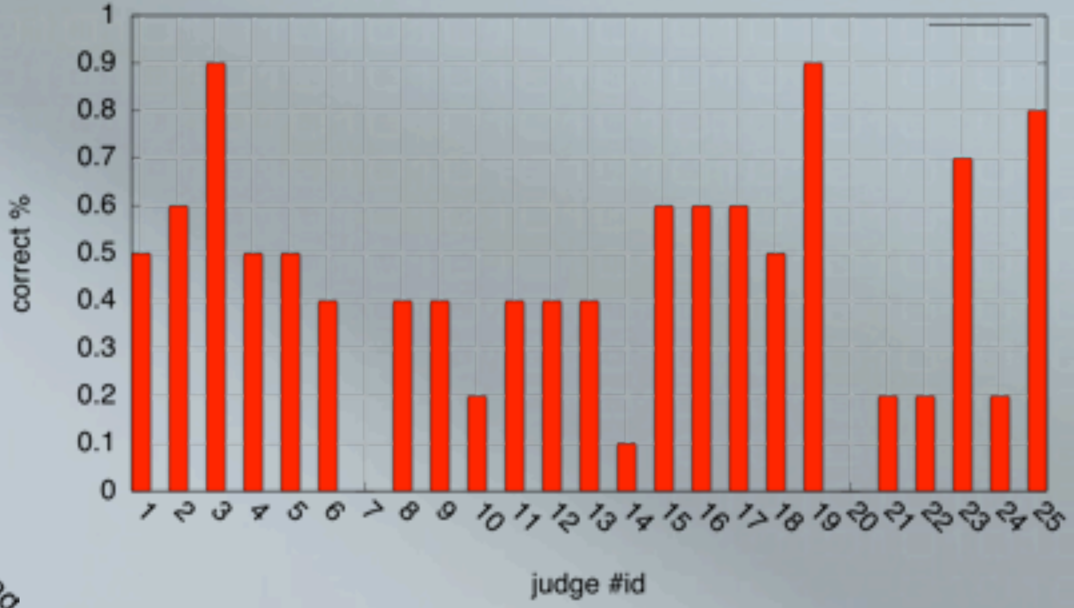
Decoy Turing Test

- Goal is to measure the believability of the simulations
- 25 human judges, consisting of security-minded PhDs, graduate-level students, and security professionals
- Tasked with observing a set of 10 videos that capture typical user actions performed on a host and make decision about each video: real or simulated

Decoy Turing Test Results

- The overall success rate was ~46%
- Graphs show results for each of the 5 scenarios and each of the 25 judges



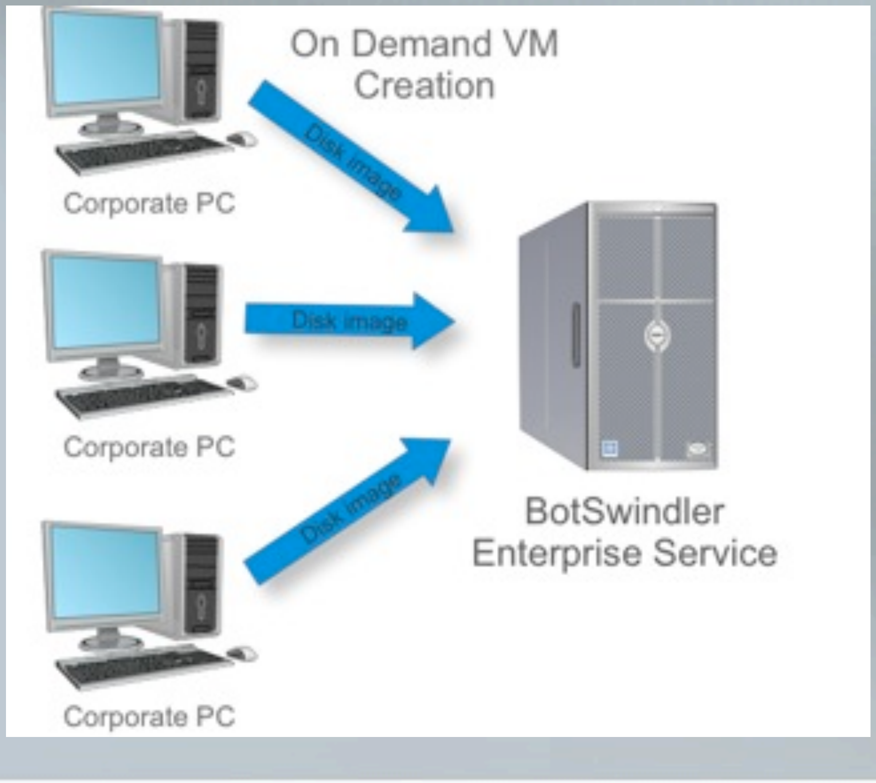


Experiments with malware

- Subscribed to an active feed of binaries at the Swiss Security blog and Offensive Computing for Zeus variants
- 5 PayPal and 5 Gmail decoys
- Phony PayPal site to give accounts enticing attributes (balance, verification, etc)
- 20 minute simulation for each binary
- Results: 13 PayPal and 1 Gmail alert

Conclusion – Future Work

- Extending BotSwindler
  - Investigate methods for automating the porting of simulations from one host to another – enable enterprise service
  - Additional experiments with real bank accounts with real balances and tracking within the UE working collaboratively with an external organization (team Cymru)



Conclusion

- Different insiders pose different types of risks and a range of factors distinguishes them.
- There is no simple solution -> use an arsenal of tools for a layered defense
  - Policies
  - Behavior based
  - Trap-based
- Trap-based mechanisms can be effective
- Lack of data makes research especially difficult

Approved References

- [1] Adreolini, M., Bulgareli, A., Colajanni, M., Mazzoni, G., “HoneySpam: honeypots fighting spam at the source,” Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop, Cambridge, MA, 2005.
- [2] [BZP06]Borders, K., X. Zhao, and A. Prakash. ”Siren: Catching the Evasive Malware (Short Paper),” Proceedings of the 2006 IEEE Sumposium on Security and Privacy, 2006.
- [3] [BA04] Brackney, R. C., and Anderson R. H., “Understanding the Insider Threat,” Proceedings of the March 2004 Workshop, RAND National Security Research Division, 2004.
- [4] McCormick, M., “Data Theft: A Prototypical Insider Theft”, Proceedings of the first Workshop on Insider Attack and Cyber Security, Washington DC, June 2007.
- [5] [CMST06]Moore, A. P., Cappelli, D., Randall, T. F., “The Big Picture of Insider IT Sabotage Across U.S. Critical Infrastructures, CERT, Software Engineering Institute and CyLab at Carnegie Mellon University, 2007
- [6] Cappelli, D., Moore, A., Shimeall, T., Trzeciak, R., “Common Sense Guide to Prevention and Detection of Insider Threats”, Carnegie Mellon University, 2006.
- [7] Chinchani, R., Muthukrishnan, A., Chandrasekaran, M., “RACOON: Rapidly Generating User Command Data for Anomaly Detection from Customizable Templates”, 2004.
- [8][CCU06] Chandrasekaran, M., Chinchani, R., Upadyaya, S., “Phoney: Mimicking User Response to Detect Phishing Attacks”, Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks, 2006.
- [9] [CW87] Clark, D. D. and Wilson, D. R., “A Comparison of Commercial and Military Computer Security Policies”. IEEE Symposium on Security and Privacy, 1987.

Approved References

- [10] Hu, Y., Zhichun, X., Brajendra, P., “Modeling Deceptive Information Dissemination Using a Holistic Approach”, SAC ’07, March, 2007.
- [11] Hu, Y., Zhichun, X., Brajendra, P., “A Trust Based Information Dissemination Model for Evaluating the Effect of Deceptive Data”, Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS ’07), 2007.
- [12] Krishnamurthy B., “Mohunk: mobile honeypots to trace unwanted traffic early”, Applica- tions, Technologies, Architectures, and Protocols for Computer Communication, Proceedings of the ACM SIGCOMM workshop on Network troubleshooting: research, theory, and opera- tions practice meet malfunctioning reality, Portland, Oregon, 2004.
- [13] The Honeynet Project, “Know Your Enemy: Sebek, A Kernel based data capture tool”, November, 2003.
- [14] [MS05] Maloof, M. and Stephens, G. D., “ELICIT: A System for Detecting Insiders Who Violate Need-to-know”. Recent Advances in Intrusion Detection (RAID), 2007.
- [15] [May05] Maybury M., et. Al., Analysis and Detection of Malicious Insiders, 2005. https://analysis.mitre.org/proceedings/Final_Papers_Files/280_Camera_Ready_Paper.pdf
- [16] [NRK01] Nguyen, N., Reiher, P., Kuenning, G. H., “Detecting Insider Threats by Monitoring System Call Activity”, Proceedings of the 2003 IEEE Workshop on Information Assurance, 2003.
- [17][MV07] McRae, Craig M. and Vaughn, Rayford B. “Phighting the Phisher: Using Web Bugs and Honeytokens to Investigate the Source of Phishing Attacks”, Proceedings of the 40th Hawaii International Conference on System Sciences, 2007.
- [18] Michael, J. B., Auguston, M., Rowe, N. C., Riehle, R. D., “Software Decoys: Intrusion Detection and Countermeasures”. Proceedings of the 2002 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2002.

Approved References

- [19] [PSU04] Pramanik, S., Sankaranarayanan, V., Upadhyaya, S., “Security Policies to Mitigate Insider Threat in the Document Control Domain”, Proceedings of the 20th Annual Computer Security Applications Conference, IEEE Society, Washington, DC, 2004.
- [20] Qutaibah, A., Brajendra P., “Knowledge Extraction and Management for Insider Threat Mit- igation”, WOSIS, 2008.
- [21] Rowe, N. C., “Measuring Effectiveness of Hoenypot Counter-deception”, HICSS ’06: Pro- ceedings of the 39th Annual Hawaii International Conference on System Sicences, Volume 05, IEEE Computer Society, 2006.
- [22] Rowe, N. C., “Designing Good Deceptions in Defense of Information Systems”, ACSAC ’04: Proceedings of the 20th Annual Computer Security Applications Conference, IEEE Computer Society, 2004.
- [23] Spitzner, L., “Honeypots: Catching the Inisder Threat” Proceedings of ACSAC. Las Vegas, December, 2003.
- [24] Spitzner, L., “Honeytokens: The Other Honeypot”, Security Focus, 2003.
- [25] Stoll, C. The Cuckoo’s Egg, Doubleday, 1989. NOT USING
- [26] [Yuill 04]Yuill, J., Zappe M., Denning D., and Feer F.. “Honeyfiles: Deceptive Files for Intrusion Detection”, Proceedings of the 2004 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY, June 2004.
- [27] [Yuill 06]Yuill, J., D. Denning, Feer, F., “Using Deception to Hide Things from Hackers : Processes, Principles, and Techniques”, Journal of Information Warfare, 5(3): 26-40, November, 2006.
- [28] Costa et al, “DTB Project: A Behavioral Model for Detecting insider Threats”, 2005. https://analysis.mitre.org/proceedings/Final_Papers_Files/260_Camera_Ready_Paper.pdf

Approved References

- [29] Webb, S., Caverlee, J., Pu, C., “Social Honeypots: Making Friends with a Spammer Near You”, Conference on Email and Anti-Spam, Microsoft Researc Silicon Valley, Mountain View, CA, 2008. http://www.ceas.cc/2008/papers/ceas2008-paper-50.pdf
- [30] [ZN00] Zadok, E., Nieh, J., “FIST: A Language for Stackable File Systems”, Proceedings of 2000 USENIX Annual Technical Conference. San Diego, CA, June, 2000.