Insider Threats:

Challenges and Mitigation Approaches

James Joshi

Professor, Director of LERSAIS

School of Computing and Information,

University of Pittsburgh

SEI-CERT: definition of Insider Threat

- "a current or former employee, contractor, or business partner who meets the following criteria:
  - has or had authorized access to an organization's network, system, or data
  - has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems"
  - has no malicious intent associated with his or her action (or inaction) that cause harm or substantially increase the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems."

Insider threat: agents/actors or influences

- Employees
  - Current and terminated
  - Remote employees
- Partners
  - Contractors/Sub-contractors
  - Outsourced companies
  - Third party Vendors
- Outside collaborations -> collusions
- Mergers and acquisitions
- ….

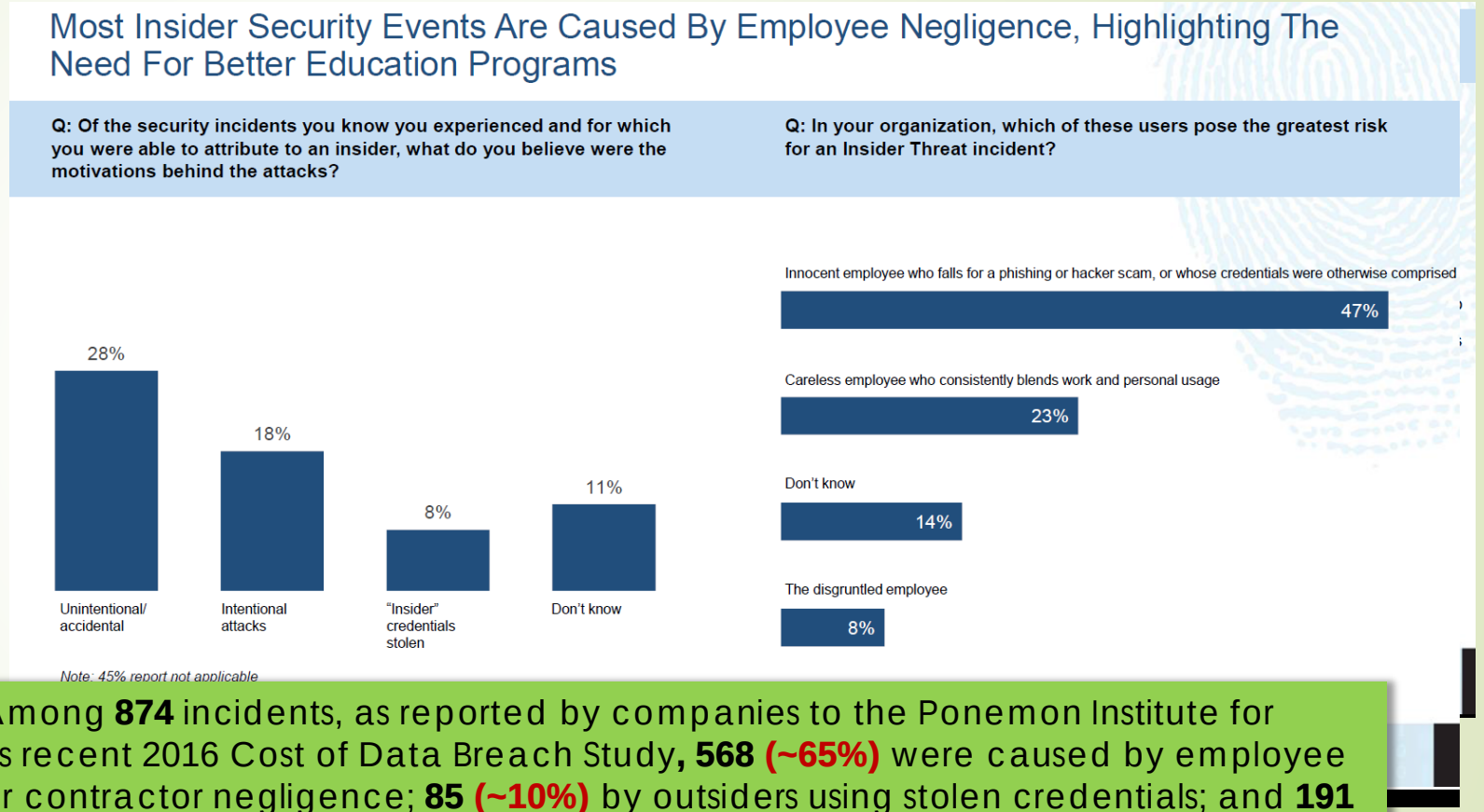
- Exploitation of an opportunity
- Revenge by disgruntled
- Political or social statement
- For competitors (blackmail/bribery)
- ….

- Compromise network security,
- Breach databases,
- Disable security controls,
- Install malware,
- Exfiltrate data,
- Aid adversarial multi-vector information warfare and
- Waste critical resources
- ……

humans remain the weakest link in an organization’s cybersecurity

Insider Threat types

- Malicious
  - Sabotage,
  - IP Theft,
  - Espionage,
  - Fraud (financial gain)
- Non-Malicious
  - Negligent users
    - intentionally neglect
    - Misguided activities
  - Untentionanal
    - Human error,
    - Bad judgement,
    - Phishing,
    - Malware
    - Stolen Credentials



Among **874** incidents, as reported by companies to the Ponemon Institute for its recent 2016 Cost of Data Breach Study**, 568 (~65%)** were caused by employee or contractor negligence; **85 (~10%)** by outsiders using stolen credentials; and **191 (~22%)** by malicious employees and criminals.

Source: 2017 US State of Cybercrime Survey, conducted by CSO, US Secret Service, Carnegie Mellon University CERT, and Forcepoint.

Some more data ...

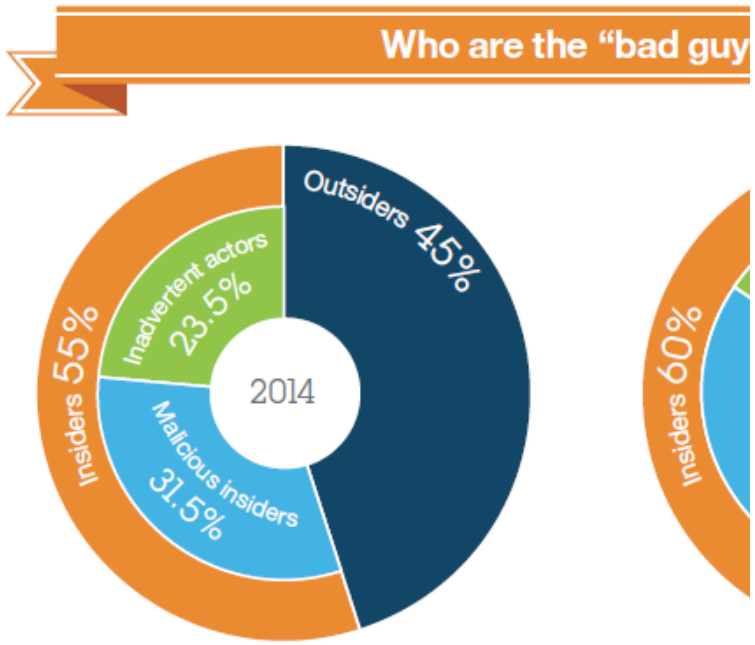


Figure 4. In 2015, outsiders were found to be responsible f
recorded, while 60 percent of attacks were carried out by
organizations' systems.

Attack sources by industry

1 January 2016 through 31 December 2016

	Industry sector	% Malicious insider	% Inadvertent actor	% Outsiders
1	Financial services	5%	53%	42%
2	Information and communications	1%	3%	96%
3	Manufacturing	4%	5%	91%
4	Retail	2%	7%	91%
5	Healthcare	25%	46%	29%

Fewer

More

58%

71%

Figure 9: Attack sources by industry – 1 January 2016 through 31 December 2016.

Example insider attacks

"The year 2013 may be the year of the insider threat. … These incidents highlight the need to improve the ability of organizations to detect, deter, and respond to insider threats".

Edward Snowden ▪ Computer Emergency Response Team (CERT), **January 2014**.

- NSA & WikiLeaks
- Target Breach in 2013
  - Estimated $1B

- Sony hack in 2014
  - North Korea or Disgruntled Insider? Stolen credentials? Phishing emails?
- Stuxnet – through infected USBs … exploitation of insiders
  - contractors to reach the target (https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/)
- 2011 - Wastewater utility in Mesa, AZ (mannal shut-down of OS)
- 2000, a contract employee - disgruntled – in Australian wastewater services company, attacked the facility's supervisory control and data acquisition (SCADA) systems
  - disabled system functions and allowed a total of 800,000 liters of untreated sewage to spill into receiving waters over a period of several weeks.

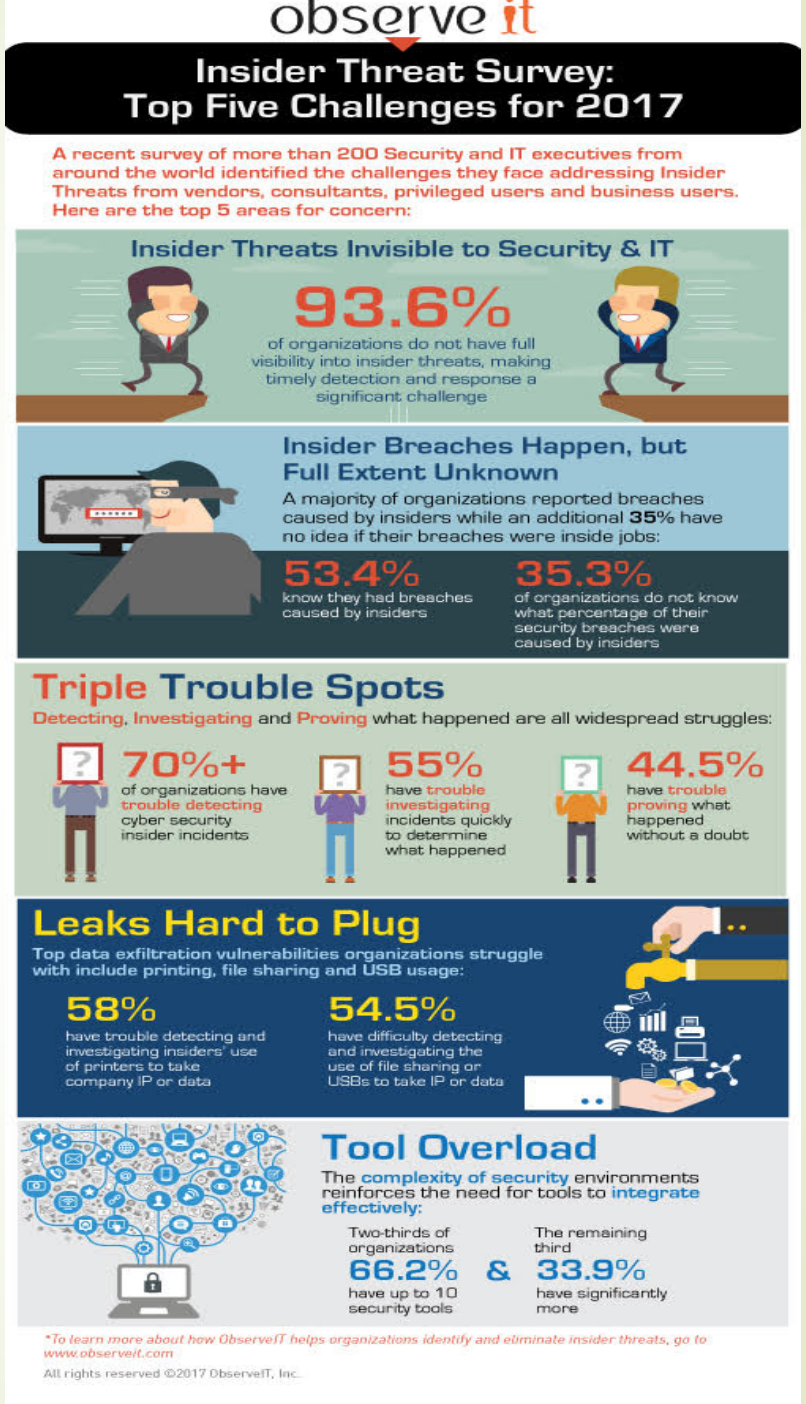
Source: https://www.esecurityplanet.com/network-security/researchers-say-sony-hack-was-insider-breach.html

https://www.tripwire.com/state-of-security/latest-security-news/sony-hackers-used-phishing-emails-to-breach-company-networks/

Challenges

"Insider threats are influenced by a combination of technical, behavioral, and organizational issues and must be addressed by policies, procedures, and technologies"

"humans remain the strongest and the weakest link in every organization's cybersecurity"



Invisibility

Coverage

DIP

Exfiltration control

Overlaod

Expanding threat environment

- The WEF 2017 Global Risks Report : "**cyberattacks, software glitches, and other factors could spark systemic failures that "cascade across networks and affect society in unanticipated ways**."

Source: Key findings from The Global State of Information Security® Survey 2018

- Current and emerging ..
  - Mobile technologies
  - Social Networks
  - Internet of Things
  - Cloud computing
  - Big data
  - ...

Increasing:
- Complexity
- Connectivity
- Pervasiveness

& Constantly
- Evolving

Mitigation Approaches

- Some key issues
  - Human issue is central !!
    - Behavioral monitoring vs. Privacy
  - Existing approaches are typically REACTIVE
  - **Can we predict**?

Insider attacks are typically preceded by **technical** and **psychological precursors**

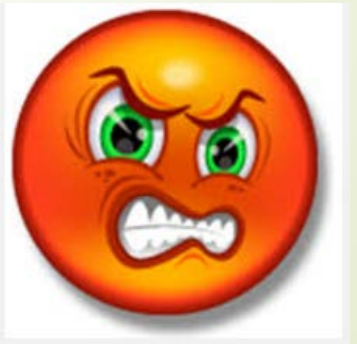
Mitigation Approaches

- Design & Implement appropriate security programs
  - Procedures and policies
  - Risk Management
  - Security education, training and awareness program (SETA)
- Design Adequate Access Control policies and solutions
- Predict attack: Monitoring and anomaly detection
  - Detect undesirable changes in behavior and tune up security controls

Technical & Psychological precursors

- Download and use of hacker tools
- Access to other users' or customer data (misuse)
- Setup or use of backdoors
- Transmitting large files
- Etc.

- Disgruntlement
- Bad attitude
- Lack of dependability
- Absenteeism
- Etc.



[Greitzer et. al]

Access Control System

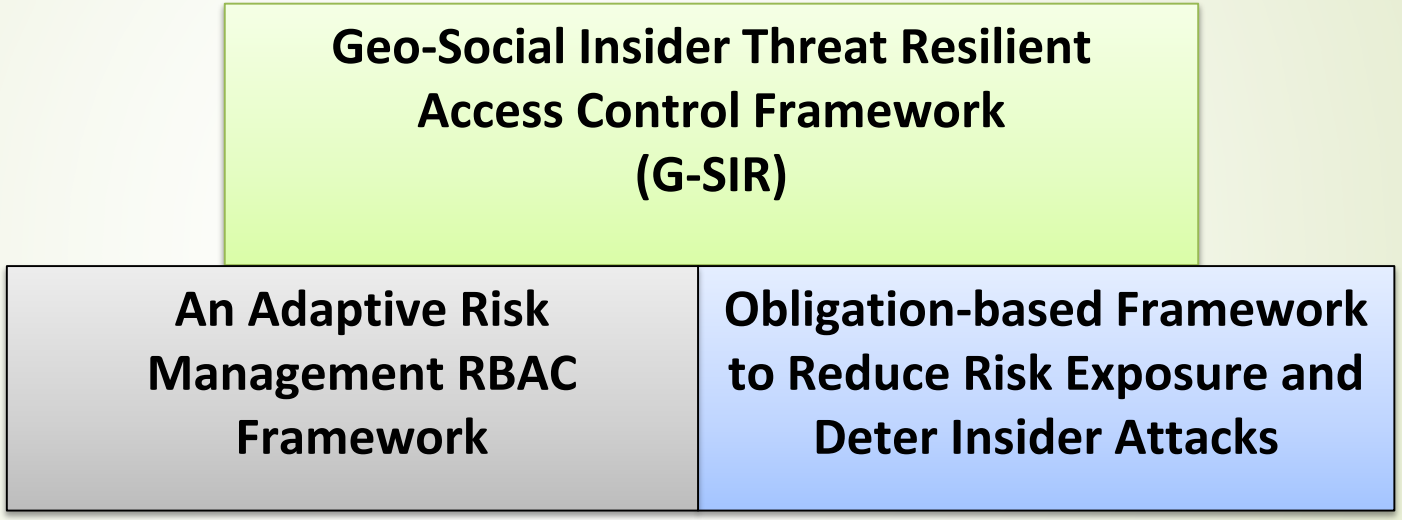
- This is a MUST!
- Restrict the access enforcing
  - Separation of duty
  - Least privilege enforcement

- **Challenge**: Employees need the privileges, but we need to prevent the abuse those permissions

Current Access Control Approaches

- Access control systems are highly static
  - As long as users have the required credentials, they can access the system
  - What about their behavior?
- Require manual verification and input
  - Manual verification of alerts
  - Input of psychological precursors is slow and subjective

Our proposed adaptive access control approach



Nathalie Baracaldo, "Tackling Insider Threats Using Risk-and-Trust Aware Access Control Approaches". 2016. **PhD Thesis**. *University of Pittsburgh.*

Joint work

Nathalie Baracaldo, Balaji Palanisamy, James Joshi. "G-SIR: An Insider Attack Resilient Geo-Social Access Control Framework," *IEEE Transactions on Dependable and Secure Computing*, IEEE, 2017

Nathalie Baracaldo, James Joshi "An Adaptive Risk Management and Access Control Framework to Mitigate Insider Threats" *Computers & Security*. 2013.(Journal)[

Nathalie Baracaldo, James Joshi "Beyond Accountability: Using Obligations to Reduce Risk Exposure and Deter Insider Attacks" *ACM Symposium on Access Control Models and Technologies (SACMAT)*, Amsterdam, The Netherlands. 2013.

Nathalie Baracaldo, James Joshi "A Trust-and-Risk Aware RBAC Framework: Tackling Suspicious Changes in User's Behavior" *ACM Symposium on Access Control Models and Technologies (SACMAT)*, Newark, USA. 2012.

1. An Adaptive Risk Management RBAC Framework

We identify an opportunity to control risk frequently (for each access request) and automatically ☺

- Two concepts:
  - **Trust:** expectation of future behavior based on the history
  - **Risk:** likelihood of a hazardous situation and its consequences if it occurs
- We include **risk** and **trust** in access control systems to adapt to anomalous and suspicious changes in users' behavior

Requirements

1. Enforce separation of duties (SoD) and cardinality constraints
2. Detect suspicious activities, and establish a trust level for each user
   - Different trust values for users depending on the *context*
3. Different permissions may have different risks associated with them
   - Adapt to suspicious changes in behavior of users by restricting permissions depending on risk values
4. Risk exposure should be **automatically** reduced, minimizing the impact of possible attacks

In a nutshell...

role

permission

trust_threshold(role)

authorized(*u*,role) & trust(u,c)≥trust_threshold(role)

Trust value of users

- Each user u is assigned a trust value:
  - $0 \leq trust(u,c) \leq 1$ → reflects his **behavior**
  - Where *c* is the context, and *u* is the user
- Some works exist to calculate this value

Assigning risk to permissions

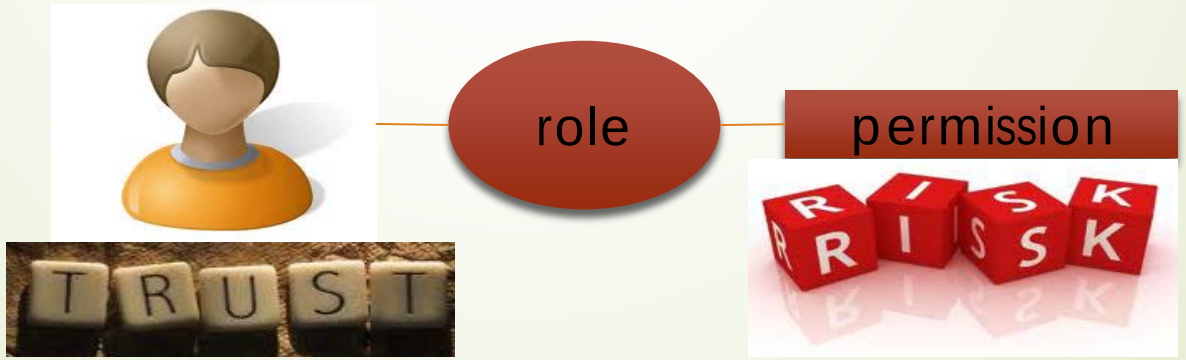
- Each permission is assigned a risk value according to:
  - The *context*
  - The likelihood of misuse
  - The cost of misuse

DEFINITION 1. *The risk of permission* $p = \langle obj, act \rangle \in P$ *in context* $c \in C$, *written as* $rs(p, c)$, *is defined as follows:*

$$rs(p, c) = \sum_{x_p \in MaliciousUsage} Pr[x_p |\ c\ ] * \mathcal{C}(x_p)$$

Risk of roles

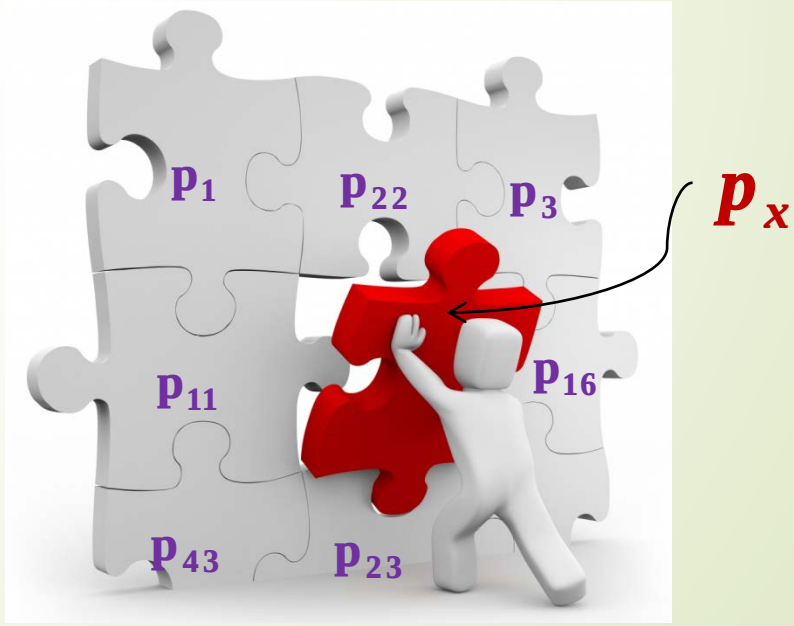
- The risk of activating a set of roles depends on:
  - Context
  - The user that is going to activate the roles
  - Authorized permissions & their risk
  - Inference risk



Inference risk

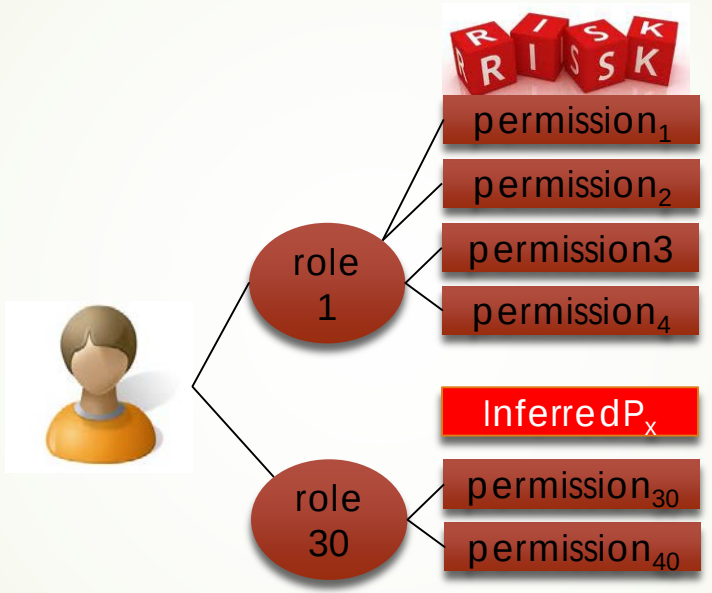
- *Inference Threat:* exists when a user is able to infer unauthorized sensitive information through what seems to be innocuous data he is authorized for
- *Inference tuple:* <*PS*, p_x>

  Shows the minimum information needed (*PS*) to infer p_x



Risk of roles

- Risk exposure of activating a set of roles

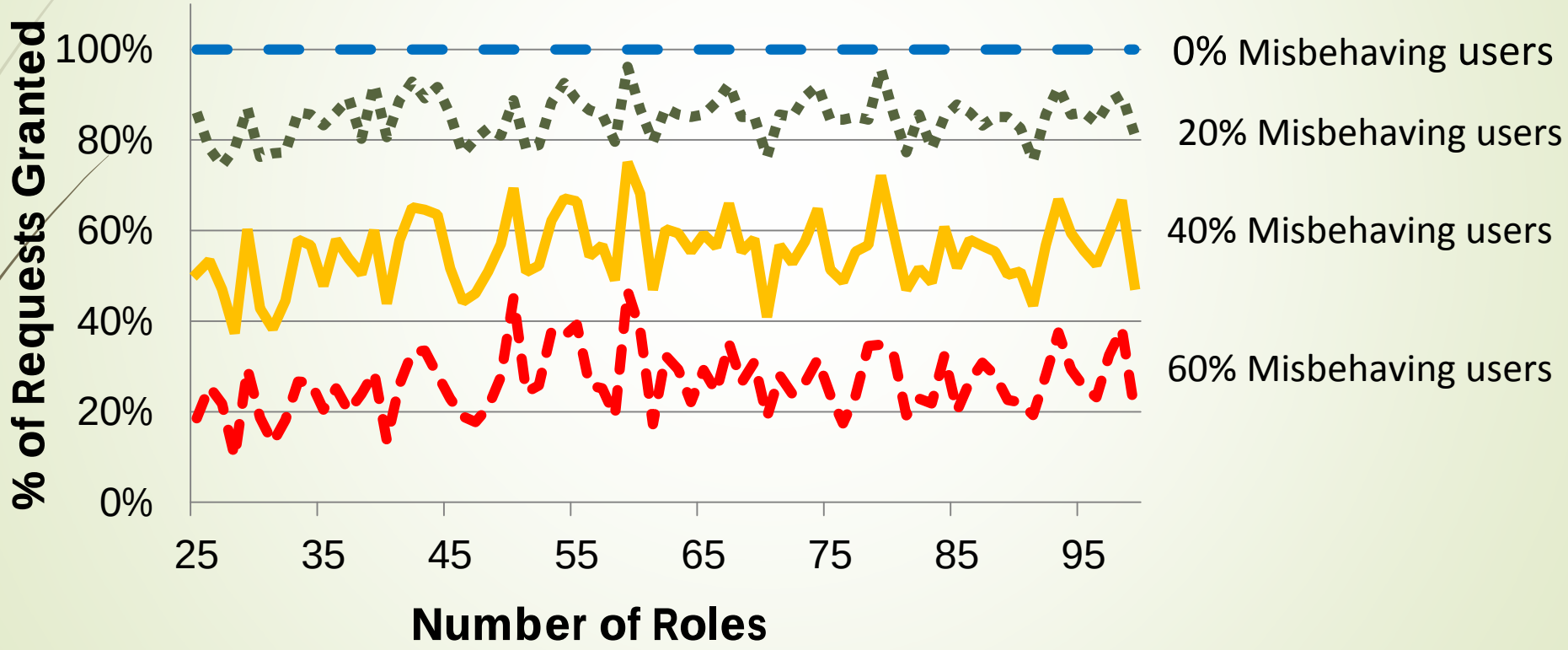


- For a set of roles *RS*, the **trust threshold** is the normalized version of their risk
- $0 \leq trust\_threshold(RS, c, u) \leq 1$

Experimental Setup

- We generated synthetic *well-formed policies*
- Each point represents the average time of running the algorithm for 30 different policies
- We evaluated our algorithm under two different heuristics for several types of policies

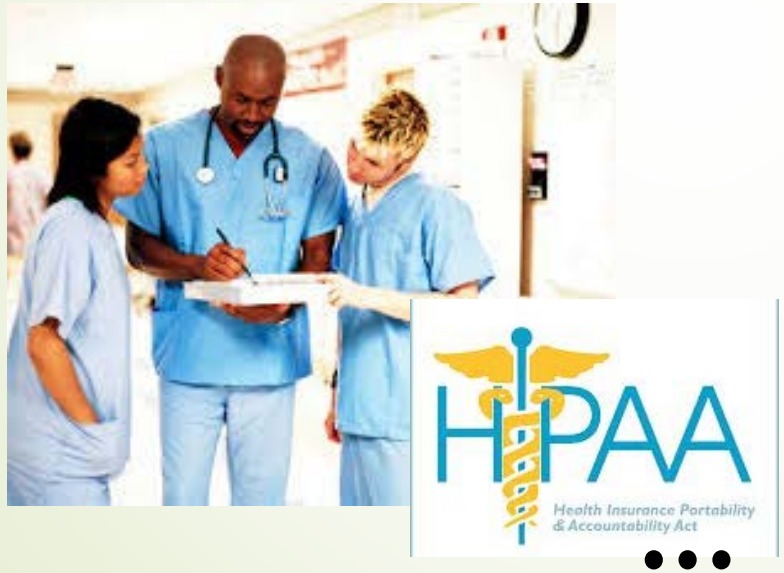
Granted requests for different percentage of misbehaving users



Critical accesses are denied preventing possible attacks

2: Obligation-based Framework To Reduce Risk Exposure And Deter Insider Attacks

- Many application domains require the inclusion of **obligations** as part of their access control policies



...

Managing *a posteriori* obligations is challenging

- Once you grant access to a user, there is **no guarantee** that he will fulfill the associated obligation
- Statistics show that it is not wise to trust users blindly!

Ideally

But this may happen

Especially because

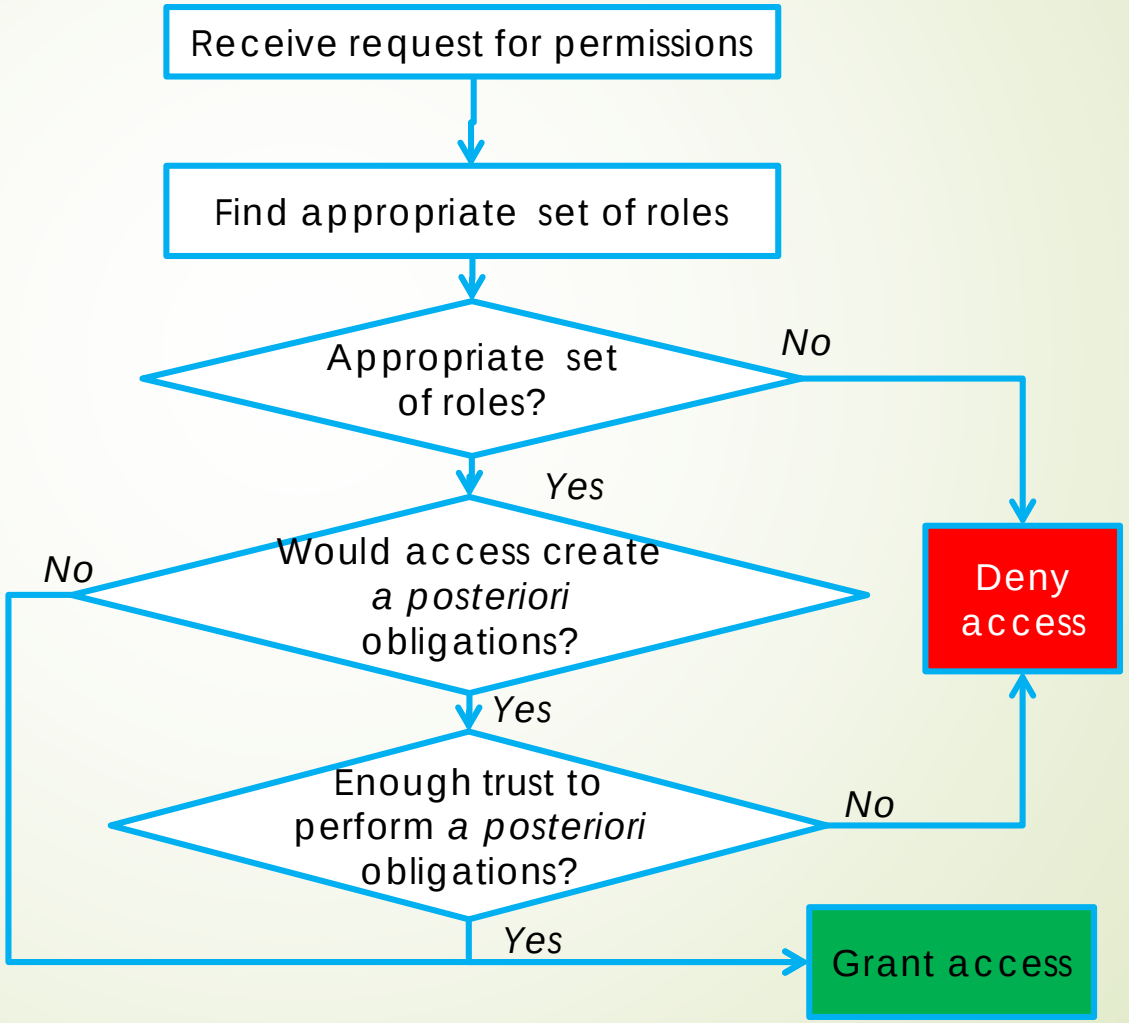
- Every time an ***a posteriori*** obligation is assigned to a user, there is some risk of non-fulfillment
- The **risk exposure** depends on the impact of not fulfilling the obligation
  - Delays on the operation
  - Fines
  - Loss of good will
  - Lawsuits

Requirements

- Reduce the **risk** exposure caused by *a posteriori obligations*
- Identify the **trust** value of a user based on the pattern of fulfillment of *a posteriori* obligations
- Identify **policy misconfigurations**
- Identify when a user is **likely** to become **an insider** attacker, without invading users' privacy

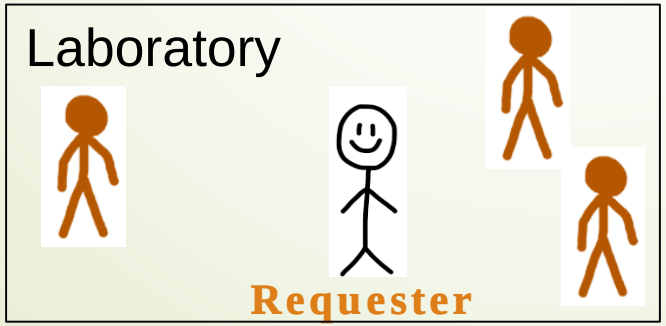
System Overview

- We use standard RBAC
- However, this trust approach can be used for any other access control model that includes obligations



3. **G-SIR:** An Insider Attack Resilient Geo-Social Access Control System

- Use location and social context to determine access
- Social graph(s)
  - Is a user part of community *X*?
  - Are two users friends?
  - What is their relationship?
  - Are they connected?



Requirements

- Classify users in the vicinity
- Design policy constraints to capture and prevent undesirable geo-social behavior: geo-social contracts, geo-social obligations and trace-based constraints
- Mitigate the risk of colluding users
- Adapt access control decisions to negative changes in behavior of users

Conclusion

- Insider threats are real and difficult to address
- Current solutions are reactive – more proactive solutions are needed
- Mitigation requires technological, policy and organization approaches
  - Significant issues related to negligence or careless users
  - SETA
- Technological and psychological percursor need to be captured
  - Adaptive security approaches can help