Insider Threats, Access Control, and Network Security

UNSW AUSTRALIA

Never Stand Still

Comp4337/9337

Guest Lecture

Dr Arash Shaghaghi

Outline

- Insider Threats
  - Definition
  - Types
  - High-risk insiders
  - Influential cases
  - Challenges in protecting against insider threats
- Detection of Insider Threats
  - Key intuition
  - Attack phases
  - Detection Approaches
- Preventing Against Insider Threats
  - Access Control
- Recent research in this area

What's wrong?!

Security model

- The term “secure” is widely abused
  - When somebody says “XYZ is secure”, ask them what they mean by the word “secure”.

- Security Model
  - **What do we want to protect?**
    - What are the conditions for the adversary to win?
  - **What resources does the adversary have?**
    - Money, computing power, …
  - **What system access does the adversary have?**
    - Insider/outsider, sees public key, wiretapping,…
  - **What is the system’s desired lifetime?**
    - 10 seconds, 1 year, infinity,…

Insider threat: non-specific to cyber

- Insider is a trusted individual who has legitimate access to resources.
- Virtually ALL cases of nuclear theft perpetrated by insiders or with the help of insiders.

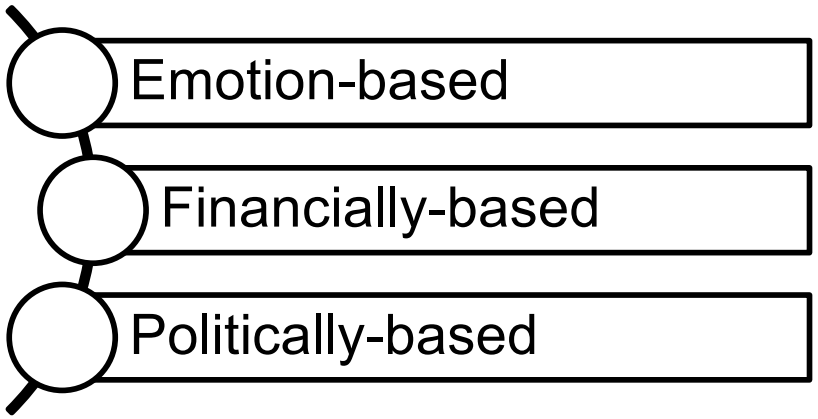
Video from **Nuclear Security & Safeguards Education Portal**
Available on YouTube: https://www.youtube.com/watch?v=Rt_80YkWo5s

Insider threat: definition

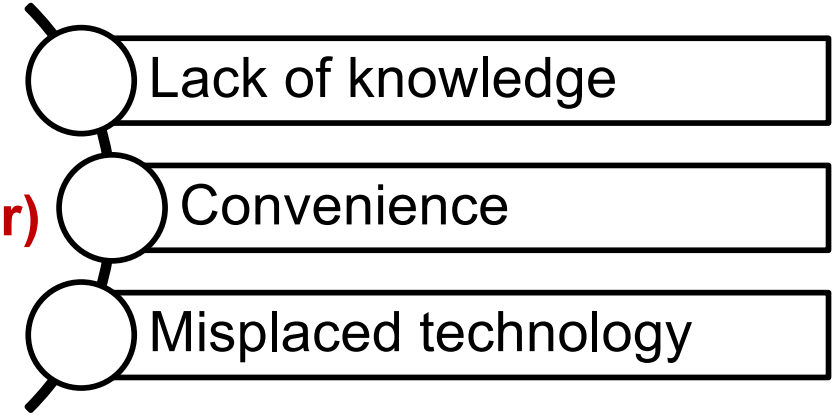
CERT : Someone who **exploits** his access to the organization's network, system, and data to take actions that negatively affect the Confidentiality, Integrity, and Availability (**CIA**) of the organization's information and Information and Communications Technology (**ICT**) infrastructure.

Types of Insiders

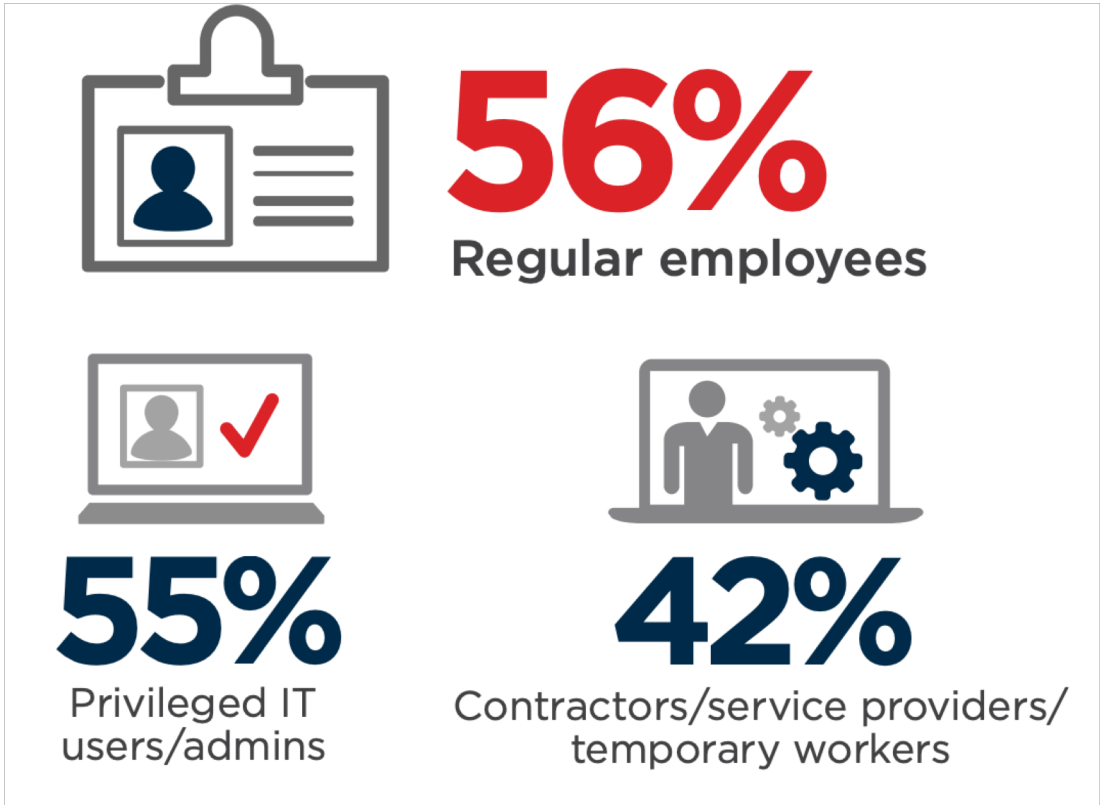
Intentional
(i.e., Malicious Insider)



Unintentional
(i.e., Non-Malicious Insider)



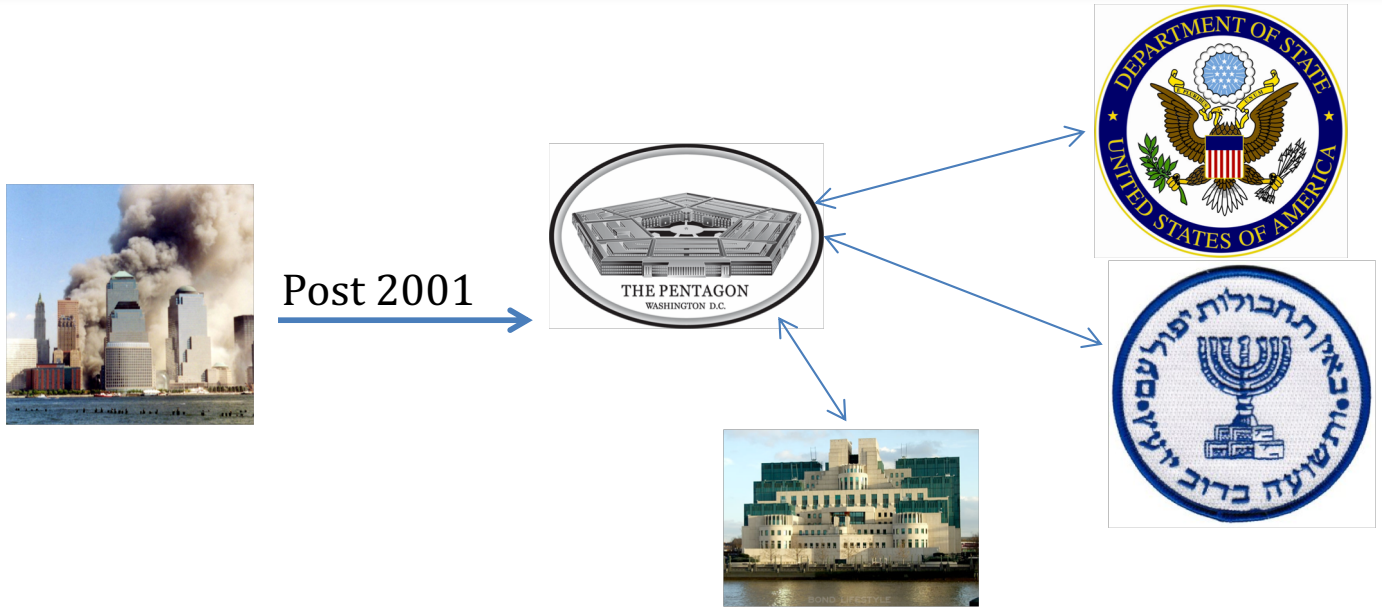
Who are the insiders?



[CA Insider Threat Report, 2018]

Cablegate: the insider threat wake-up call

Cablegate leak: the largest leak of military and diplomatic cables in U.S. history (~700,000 documents).



Post 9/11: greater sharing of information between Department of State and Defence.

How it happened?

- Private First Class Bradley E. Manning iin front of a computer at Contingency Operating Station Hammer in Baghdad, Iraq. Chatting online with an ex-hacker in San Francisco:
  - 'If you had free reign over classified networks for long periods of time... say, 8-9 months... and you saw incredible things, awful things... things that belonged in the public domain, and not on some server stored in a dark room in Washington DC... what would you do?'

Information copied to a CD-ROM (labelled as Lady Gaga), taken home, shared with WikiLeaks!!

The Snowden-case

- U.S. National Security Agency contractor
- Leaked about 200,000 classified documents about global surveillance practices and military operations.

Video from **BBC**

Available on YouTube: https://www.youtube.com/watch?v=el_WYCUHP9Y

How it happened?

Snowden smuggled out the classified documents on a thumb drive!

And continuing …

ALL of the major U.S. intelligence agencies and branches of the military have experienced an extremely damaging insider incident:

- **U.S. National Security Advisor** Sandy Berger: removed highly classified documents from the National Archives to review them at his office.
- **CIA Director** John Deutch : accessed highly sensitive classified information on an insecure computer connected to the Internet.
- **Junior employee** of Her Majesty's Revenue & Customs (**HMRC**): copied confidential records of twenty-five million individuals onto disks and sent it through the post, which got lost!

What about the less secure organizations?

%93 of US companies vulnerable to insider threats.

(Vormetric Report 2015 and 2016), …

What makes insider threats challenging?

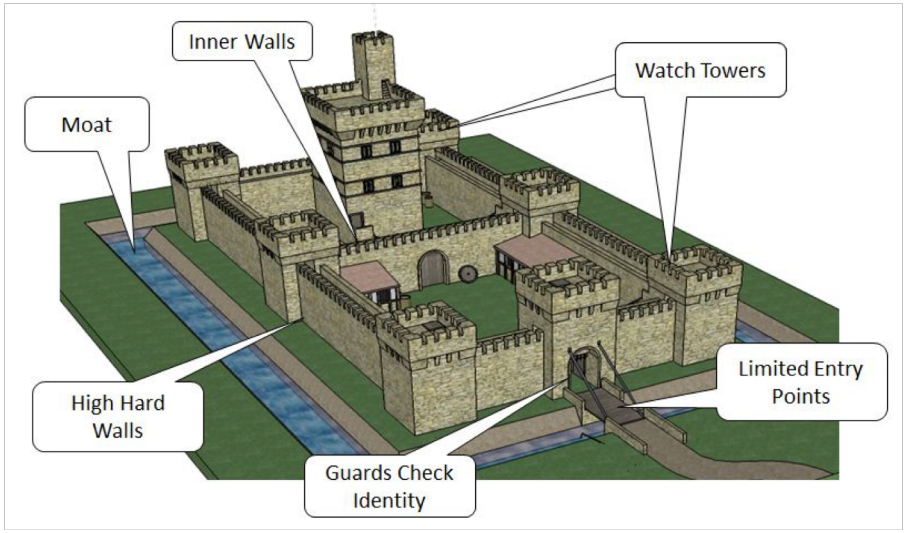
1. People/users are the weakest link.
   - *"Security is only as good as it's weakest link, and **people** are the weakest link in the chain." [Bruce Schneier, Secrets and Lies, 2000]*

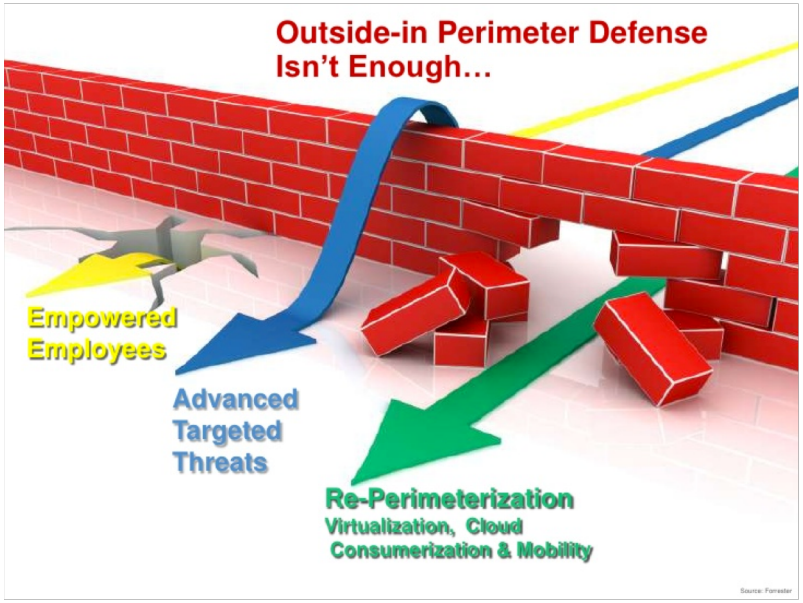
Video from **Fusion**

Available on YouTube: https://www.youtube.com/watch?v=lc7scxvKQOo

What makes insider threats challenging?

2. **Perimeter defences** are irrelevant.
   - *One who **has legitimate access** to information/systems (i.e. is trusted).*





1: http://blog.questionmark.com/wp-content/uploads/2013/02/castle2.jpg
2: https://image.slidesharecdn.com/informationsecurityexecutivesummitfeb2012-120306045535-phpapp01/95/smart-datacentric-security-for-the-postpc-era-6-728.jpg?cb=1331010636

What makes insider threats challenging?

3. Growing number of **mobile devices** with access to data and users with excessive privileges.
   - BYOD policy adopted by many organizations.
   - How easier would it be for next Snowden to copy files when accessing using own device?

WikiLeaks happened from within NSA premises.

(Snowden: “it was foolishly easy to copy information from machines”)

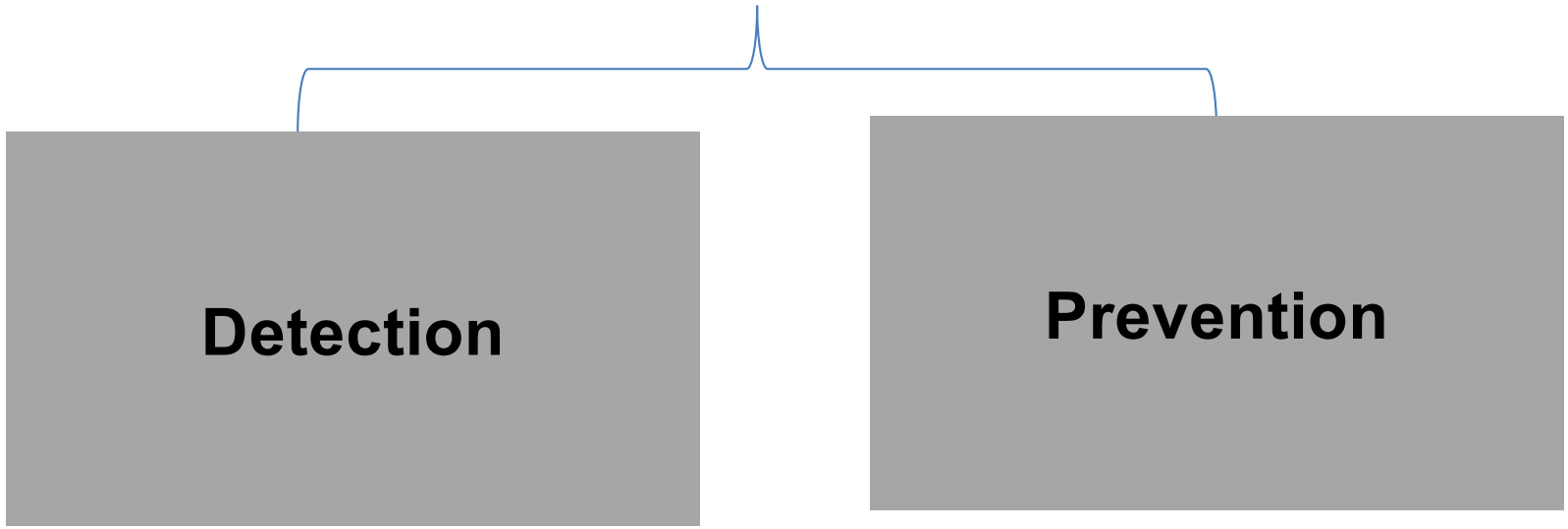
What makes insider threats challenging?

4. Still at the **early stages** of developing usable and efficient insider threat **solutions**.
   - Still more concerned about outsiders! And, not investing enough.

President Obama, **EXECUTIVE ORDER**, 2011:
implement an insider threat detection and prevention program.

Majority of organizations, still at the early stages of developing their insider threat program *[CA Insider Threat Report, 2018]*.

Protection against insider threats



How to detect: the key intuition.

- Irrespective of intent, malicious or unusual behaviour will deviate from normal behavioural patterns.

Training Video for Department of Homeland Security and Corporate Training
Available on YouTube: https://www.youtube.com/watch?v=ZAmtfNQs6JI

How to detect: the key intuition.

- Irrespective of intent, malicious or unusual behaviour will deviate from normal behavioural patterns.

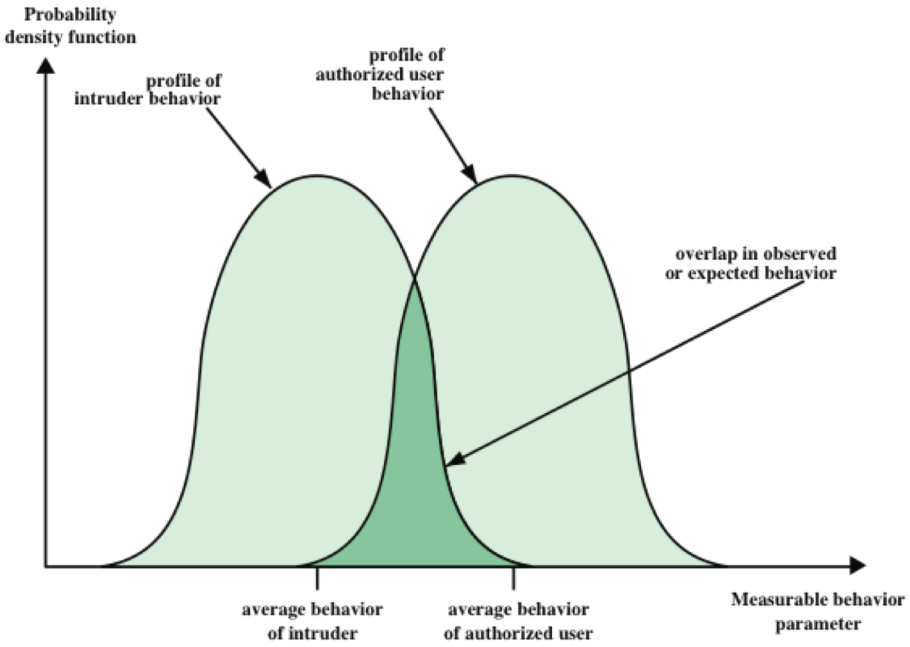


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

Figure from https://www.cse.unr.edu/~mgunes/cs450/cs450fa13/ch8_intrusion.pptx

Malicious insider attack phases

Kill chain	Threat
Reconnaissance	Port scan Network vulnerability scan Web application vulnerability scan database vulnerability scan
Weaponisation	Social engineering
Delivery	Email spam (URL or attachments) Malicious or phishing websites Removable media
Exploit	Privilege escalation
Install	RAT or backdoor
C2	DDoS Email spam Click fraud and bitcoin mining
Actions on objectives	Data exfiltration Violation against data integrity or availability Sabotage of ICT systems

Table from Liu, Liu, et al. "Detecting and preventing cyber insider threats: a survey." *IEEE Communications Surveys & Tutorials* 20.2 (2018): 1397-1417.

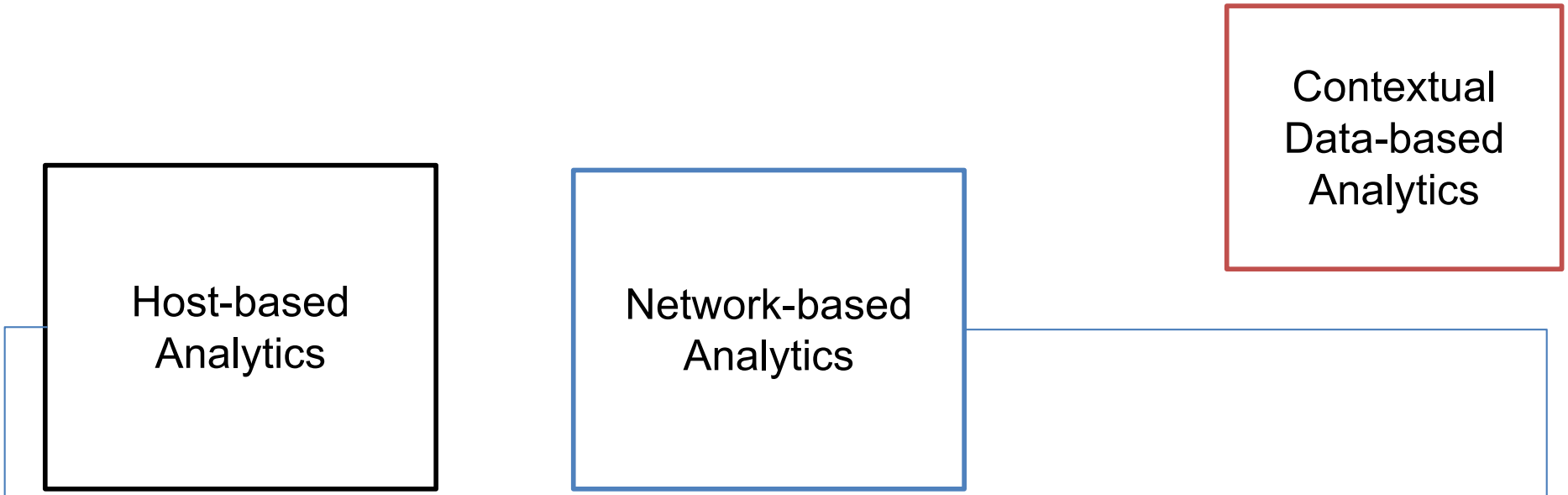
Security Attack Detection Evolution

Network perimeter firewalls, IDS, proxies, AntiVirus, DHCP, DNS
Detection technique: Signature based

Internal network, host AntiVirus, OS, application logs, email, net flow
Detection technique: Signature based + Network anomaly

Data Leak Protection (DLP), DRM, Personnel data, data object interaction, non-network data
Detection technique: Signature based + Network anomaly + Data mining, behavioral

Detection approaches



monitors the characteristics of a single host for suspicious activity

monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity

Detection approaches

Contextual Data-based Analytics

HR data, etc.

Host-based Analytics

- monitors the characteristics of a single host for suspicious activity

Network-based Analytics

- monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity.

IDS requirements

- run continually
- be fault tolerant
- resist subversion
- impose a minimal overhead on system
- configured according to system security policies
- adapt to changes in systems and users
- scale to monitor large numbers of systems
- provide graceful degradation of service
- allow dynamic reconfiguration

slide from https://www.cse.unr.edu/~mgunes/cs450/cs450fa13/ch8_intrusion.pptx

Host-based approaches to intrusion detection

anomaly detection

- threshold detection
  - involves counting the number of occurrences of a specific event type over an interval of time
- profile based
  - profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts

signature detection

- involves an attempt to define a set of rules or attack patterns that can be used to decide that a given behavior is that of an intruder

slide from https://www.cse.unr.edu/~mgunes/cs450/cs450fa13/ch8_intrusion.pptx

Data source for Host-based Analytics

- System-call
- Command, Keyboard, and Mouse
- Host log

Measure	Model	Type of Intrusion Detected
Login and Session Activity		
Login frequency by day and time	Mean and standard deviation	Intruders may be likely to log in during off-hours.
Frequency of login at different locations	Mean and standard deviation	Intruders may log in from a location that a particular user rarely or never uses.
Time since last login	Operational	Break-in on a "dead" account.
Elapsed time per session	Mean and standard deviation	Significant deviations might indicate masquerader.
Quantity of output to location	Mean and standard deviation	Excessive amounts of data transmitted to remote locations could signify leakage of sensitive data.
Session resource utilization	Mean and standard deviation	Unusual processor or I/O levels could signal an intruder.
Password failures at login	Operational	Attempted break-in by password guessing.
Failures to login from specified terminals	Operational	Attempted break-in.
Command or Program Execution Activity		
Execution frequency	Mean and standard deviation	May detect intruders, who are likely to use different commands, or a successful penetration by a legitimate user, who has gained access to privileged commands.
Program resource utilization	Mean and standard deviation	An abnormal value might suggest injection of a virus or Trojan horse, which performs side-effects that increase I/O or processor utilization.
Execution denials	Operational model	May detect penetration attempt by individual user who seeks higher privileges.
File Access Activity		
Read, write, create, delete frequency	Mean and standard deviation	Abnormalities for read and write access for individual users may signify masquerading or browsing.
Records read, written	Mean and standard deviation	Abnormality could signify an attempt to obtain sensitive data by inference and aggregation.
Failure count for read, write, create, delete	Operational	May detect users who persistently attempt to access unauthorized files.

table from https://www.cse.unr.edu/~mgunes/cs450/cs450fa13/ch8_intrusion.pptx

Network-based Analytics

Video from **Darktrace**

Available on YouTube: https://www.youtube.com/channel/UCA3MseYette-MNUSuDwrQbg

Data source for Network-based Analytics

- Network traffic
- Network logs

DNS	Network traffic (Section IV.A)
IRC & HTTP	
Netflow	
Outbound	
DNS & HTTP	
Proxy	Network log (Section IV.B)
Email & LDAP	
Web server	
Email & cell	
Proxy, Email & LDAP	
Proxy, LDAP, DHCP & VPN	
Proxy & Email	

Table from Liu, Liu, et al. "Detecting and preventing cyber insider threats: a survey." *IEEE Communications Surveys & Tutorials* 20.2 (2018): 1397-1417.

Overview of algorithms used for insider threats

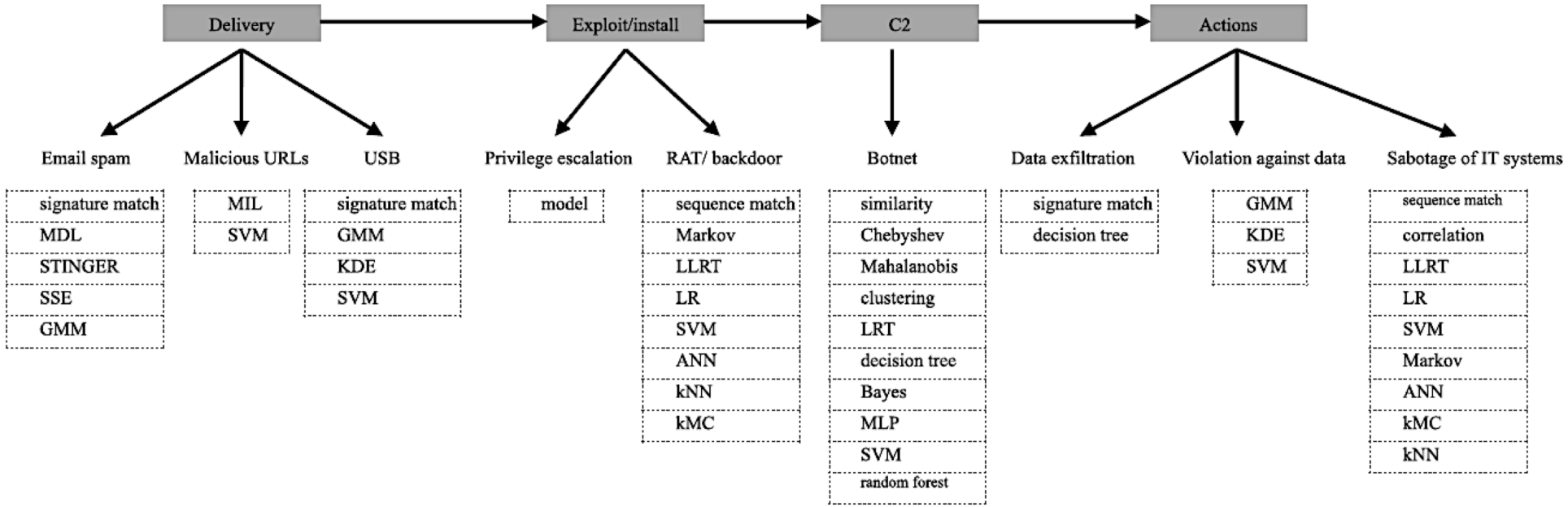
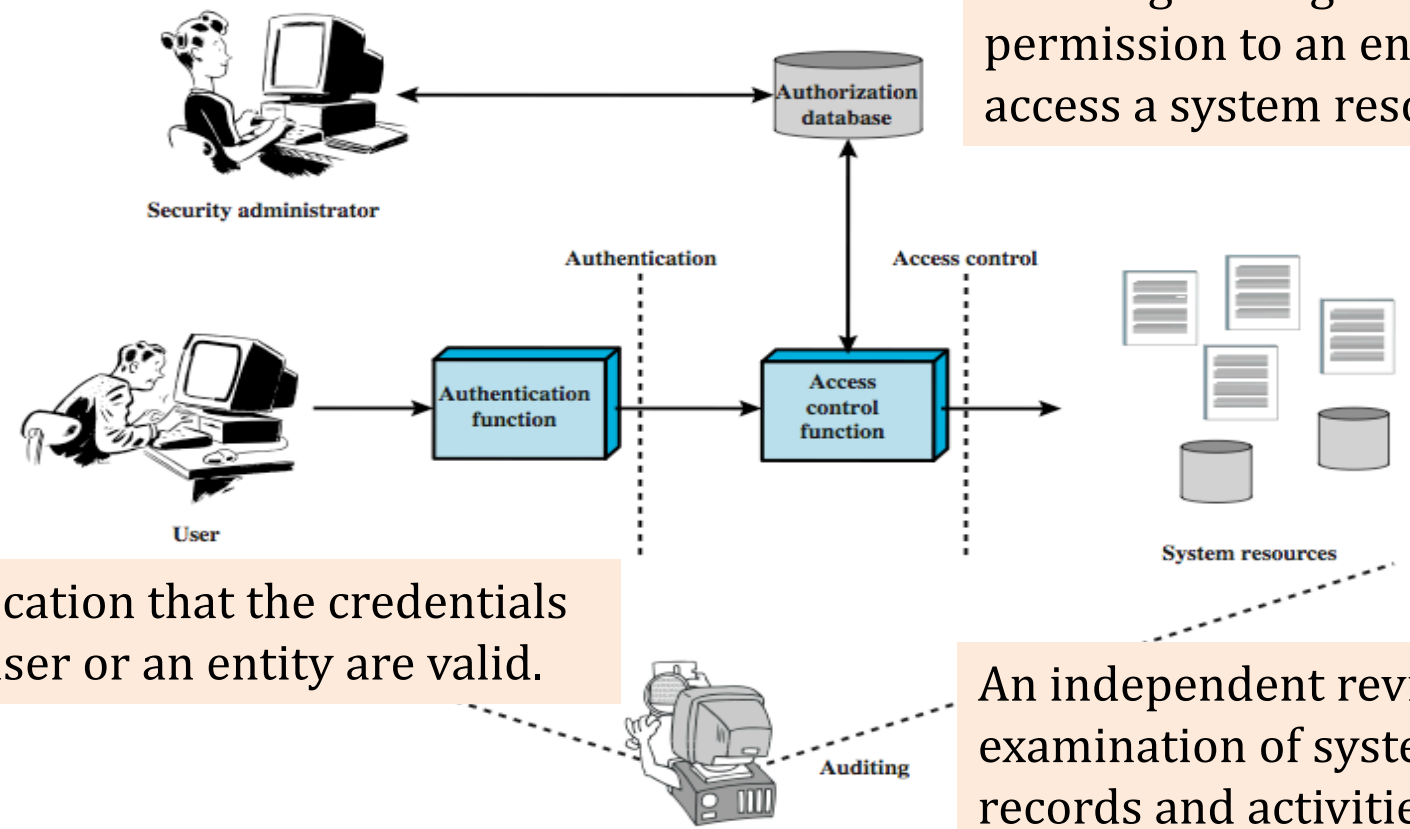


Table from Liu, Liu, et al. "Detecting and preventing cyber insider threats: a survey." *IEEE Communications Surveys & Tutorials* 20.2 (2018): 1397-1417.

Preventing insider threats

- **Access Control**: the oldest information security mechanism (pre-dates WWW).
- Who can access what, under what conditions, and for what purposes.



Granting of a right or permission to an entity to access a system resource.

Verification that the credentials of a user or an entity are valid.

An independent review and examination of system records and activities

From "Computer security principles and practice" by William Stallings, Lawrie Brown

Access control process

Subject (initiator, data requestor)	**Action** (request)	**Access Right** (permission)	**Object** (target)
• Submits the access request (e.g. the user)	• Requested Operation (e.g., read, delete, etc.)	• A specific ability for the subject to do the action to the object.	• What is being requested (e.g., a file).

Access control policies

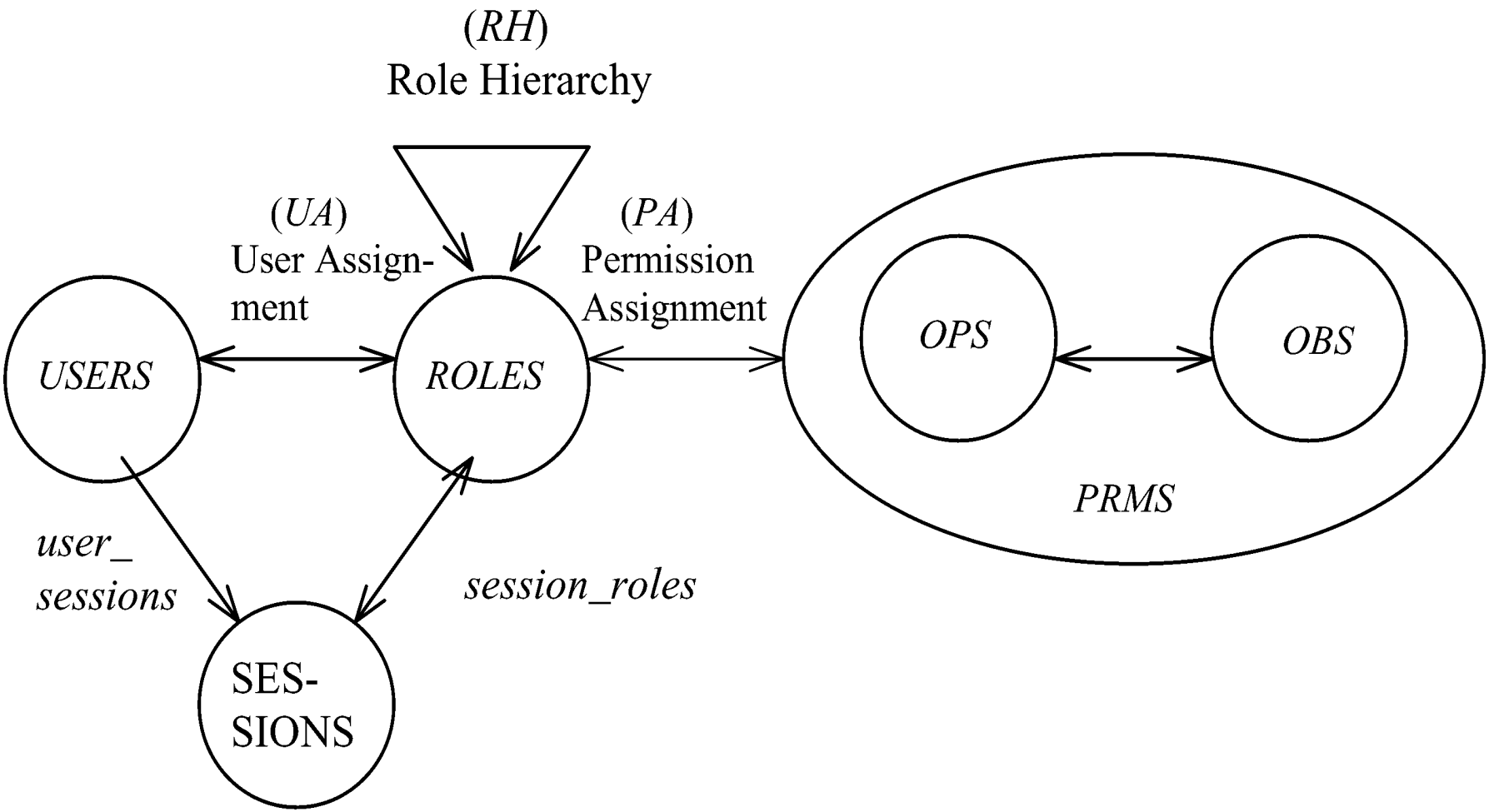
- **Discretionary Access Control (DAC)**, 1970
  - Owner controls access
  - Grounded in pre-computer policies of researchers
- **Mandatory Access Control (MAC)**, 1970
  - Synonymous to Lattice-Based Access Control (LBAC)
  - Access based on security labels
  - Labels propagate to copies
  - Grounded in pre-computer military and national security policies
- **Role-Based Access Control (RBAC)**, 1995
  - Access based on roles
  - Can be configured to do DAC or MAC
  - Grounded in pre-computer enterprise policies
  - Most commonly used model today

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

From https://profsandhu.com/miscppt/smu_abac_150410.pptx

RBAC96 model



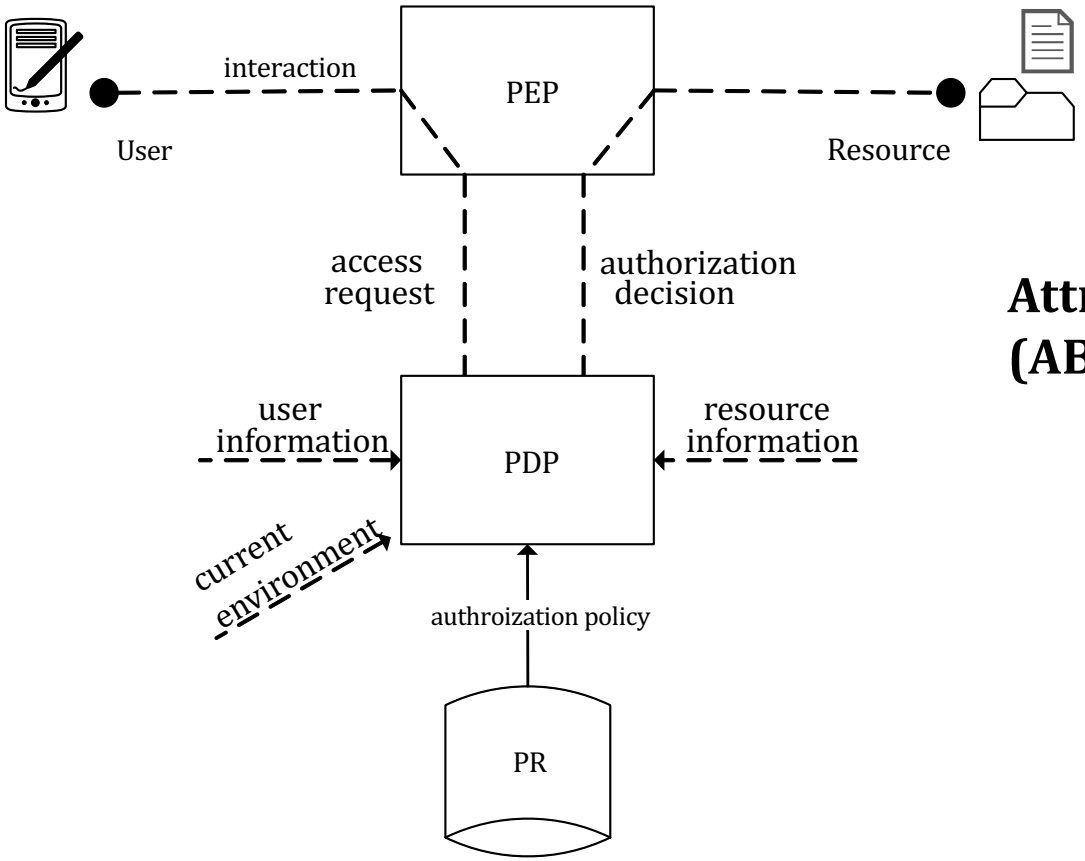
From https://profsandhu.com/miscppt/smu_abac_150410.pptx

Question

What's missing when looking at the insider attacks discussed at the beginning of this lecture? Why these were not effective in preventing those incidents?

Access CONTEXT!!

Context-based access control



Attribute-based access control (ABAC):

Based on **attributes** of the **user**, the **resource** to be accessed, and current **environment**.

By 2015,

majority of AC solutions were predicted to be context-aware in organisation *.

* Findings, K., The Future of Information Security Is Context Aware and Adaptive, 2010. Available at: http://tinyurl. com/pooswyb.

Attribute-based Access Control (ABAC)

Simple Rule Example

Any person must have the same clearance level or higher as the classification of the document he or she is requesting to view, must also be working on that project, be a current employee, and have finished the appropriate training.

A user with role==”junior” OR role==”senior” AND user.clearance>=record.classification can actionId==”view” on objectType==”record” if classification==”secret” AND user.project == “record.project” AND status==”current” and record.training is in user.training

Sample rule from https://www.axiomatics.com/blog/intro-to-attribute-based-access-control-abac/

Attribute-based Access Control

Another Rule Example

Junior personnel cannot access top secret information between 20:00 and 6:00.

```
policy checkTimeAccess {
  apply firstApplicable
   rule checkNightAccess {
    target clause role == “junior” and classification = “top secret”
    condition timeInRange(timeOneAndOnly(currentTime),
     “20:00:00”:time,  “06:00:00”:time)
   deny
   }
 }
```


Sample rule from https://www.axiomatics.com/blog/intro-to-attribute-based-access-control-abac/

XACML policy example – Cont'd

```
<Policy PolicyId="ExamplePolicy"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
  <Target>
   <Subjects> <AnySubject/></Subjects>
   <Resources><Resource>
            <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
            <AttributeValue
            DataType="http://www.w3.org/2001/XMLSchema#anyURI">http://server.example.com/code
                                    /docs/developer-guide.html</AttributeValue>
             <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#anyURI"
                        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>
            </ResourceMatch>
    </Resource></Resources>
   <Actions><AnyAction/></Actions>
  </Target>
  <Rule RuleId="ReadRule" Effect="Permit">
            ...
    </Rule>
 </Policy>
```

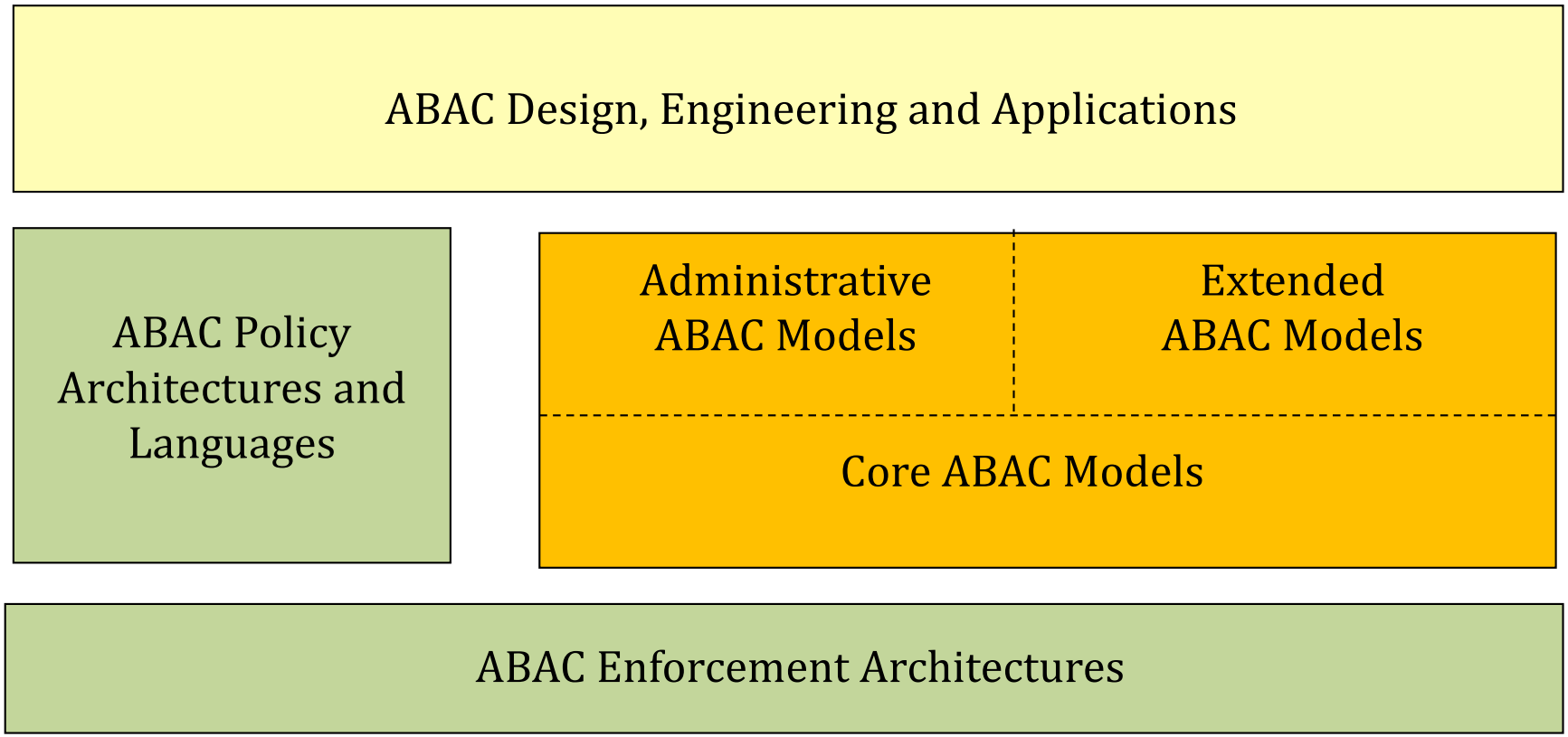

Sample XACML policy from https://ebiquity.umbc.edu/_file_directory_/resources/259.ppt

XACML policy example

```
<Rule RuleId="ReadRule" Effect="Permit">
    <Target>
        <Subjects><AnySubject/></Subjects>
        <Resources><AnyResource/></Resources>
        <Actions>
        <Action>
            <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
  DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
            <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
                AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"/>
            </ActionMatch>
        </Action>
        </Actions>
    </Target>
    <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
        <SubjectAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
                AttributeId="group"/>
        </Apply>
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">developers</AttributeValue>
  </Condition>
</Rule>
```

ABAC: an active research area

- ABAC is orders of magnitude more complex than anything that has been an Access Control.
  - Policy specification, enforcement, and implementation.



With changes from https://profsandhu.com/miscppt/darmstadt_170905.pptx

Question

What else could be missing in preventing the next insider threat?

Note: We will be referring to a few recent research work in this area by our group. Just to give you a glimpse of where the domain is headed to.

Function-based Access Control (FBAC)

Simple intuition: Model intention by **Action**.

In the case of Pentagon's access to State Department: one should be able to run data mining techniques and/or **search** documents' **without being authorized to preform any other operation** such as Print, Copy, E-mail, etc.

Contribution: Providing a systematic solution to an open problem in AC. In other words,

- **AC at level of data**,
- **Control over operation execution,** and
- **Avoid Y/N approach when making access decisions.**

Desmedt, Yvo, and Arash Shaghaghi. "Function-Based Access Control (FBAC): Towards Preventing Insider Threats in Organizations." *From Database to Cyber Security*. Springer, Cham, 2018. 143-165.

Function-based Access Control (FBAC)

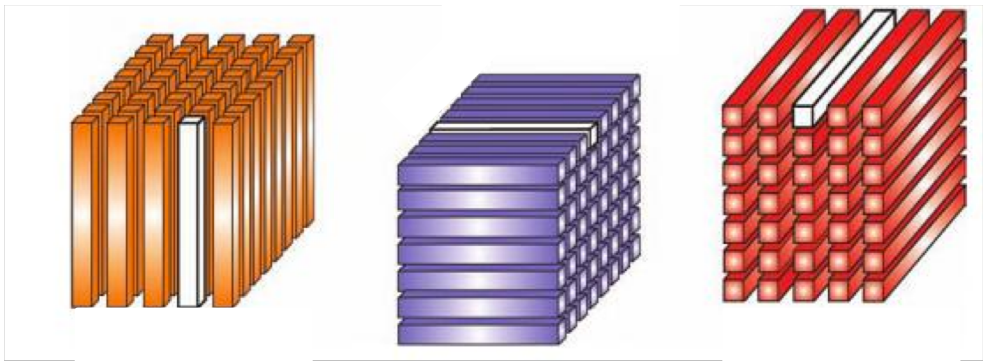
- Move from a 2-dimensional Access Control Matrix to a 3-dimensional **Access Control Tensor**.

(Subject, Object, Operation) → (Subject, Object, Function)

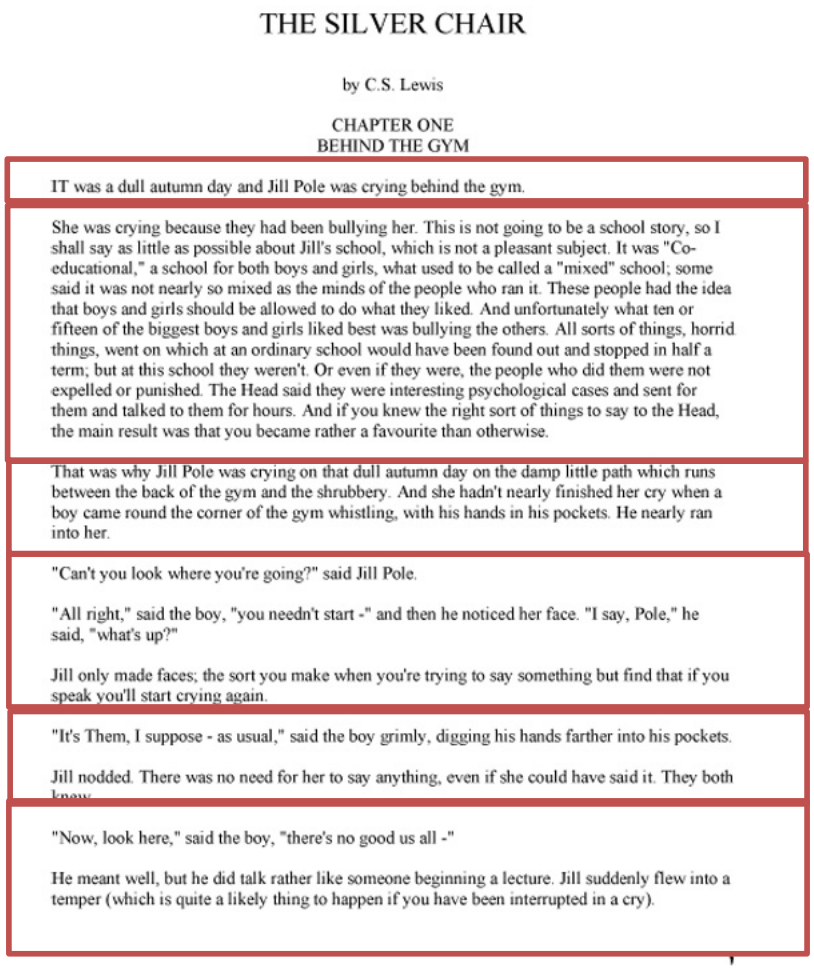
- User A can execute **Copy, Paste and Email** functions on **data blocks A and B**.

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix



Function-based Access Control (FBAC)



THE SILVER CHAIR

by C.S. Lewis

CHAPTER ONE
BEHIND THE GYM

IT was a dull autumn day and Jill Pole was crying behind the gym.

She was crying because they had been bullying her. This is not going to be a school story, so I shall say as little as possible about Jill's school, which is not a pleasant subject. It was "Co-educational," a school for both boys and girls, what used to be called a "mixed" school; some said it was not nearly so mixed as the minds of the people who ran it. These people had the idea that boys and girls should be allowed to do what they liked. And unfortunately what ten or fifteen of the biggest boys and girls liked best was bullying the others. All sorts of things, horrid things, went on which at an ordinary school would have been found out and stopped in half a term; but at this school they weren't. Or even if they were, the people who did them were not expelled or punished. The Head said they were interesting psychological cases and sent for them and talked to them for hours. And if you knew the right sort of things to say to the Head, the main result was that you became rather a favourite than otherwise.

That was why Jill Pole was crying on that dull autumn day on the damp little path which runs between the back of the gym and the shrubbery. And she hadn't nearly finished her cry when a boy came round the corner of the gym whistling, with his hands in his pockets. He nearly ran into her.

"Can't you look where you're going?" said Jill Pole.

"All right," said the boy, "you needn't start -" and then he noticed her face. "I say, Pole," he said, "what's up?"

Jill only made faces; the sort you make when you're trying to say something but find that if you speak you'll start crying again.

"It's Them, I suppose - as usual," said the boy grimly, digging his hands farther into his pockets.

Jill nodded. There was no need for her to say anything, even if she could have said it. They both knew.

"Now, look here," said the boy, "there's no good us all -"

He meant well, but he did talk rather like someone beginning a lecture. Jill suddenly flew into a temper (which is quite a likely thing to happen if you have been interrupted in a cry).

Idea in a nutshell:

Slice data files and store them as separate entities. Separate entities are called “Atom”.

We assign Function permissions for each Atom.

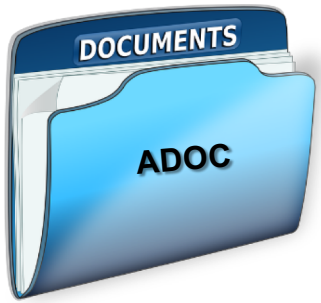
The .**ADoc** file is created on each access request by combining atoms.

.ADoc and Atoms

Each Atom has a:

Classification level

Each child Atoms has also a classification level: Classified, confidential, public, etc. The Atom classification level cannot be different from the container (.ADoc file).



$$D = \bigcup Atom(i, j, k, ...)$$

$$F(i)=\{\text{allowed functions for Atom(i)}\}$$
$$F(D)=\{\text{NOT allowed functions for Document(D)}\}$$

$$C(i)=\{\text{Classification level of Atom(i)}\}$$
$$C(D)=\{\text{Classification level of Document(D)}\}$$

$$Atom(i) \text{ is an Atom for Document(D) IFF:}$$
$$\text{C1: } F(i) \bigcap F(D) = \{\phi\} \wedge C(i) \subset C(D)$$

$$\text{Document(D) is .ADoc file complaint when:}$$
$$\forall Atom(i) \; \epsilon \; D, \text{ C1 holds.}$$

Relaxed-FBAC

1. Atom's Functions: When Atoms are created the set of Functions (F) allowed on them is specified.
2. .ADoc policy: Depending on **specified policy** a set of non-allowed functions is created for Atoms.

ATOM's Function permission list: {Copy, Paste, Email, Send to Bluetooth, Send to Wi-Fi direct, Send to messaging Apps}

.ADoc policy: If user A (member of low-level serviceman) and is after 6 PM and outside of organization safe-list zones in NY and is using APP A, or B, or C then disable Copy, Paste and Email for all atoms in this document.

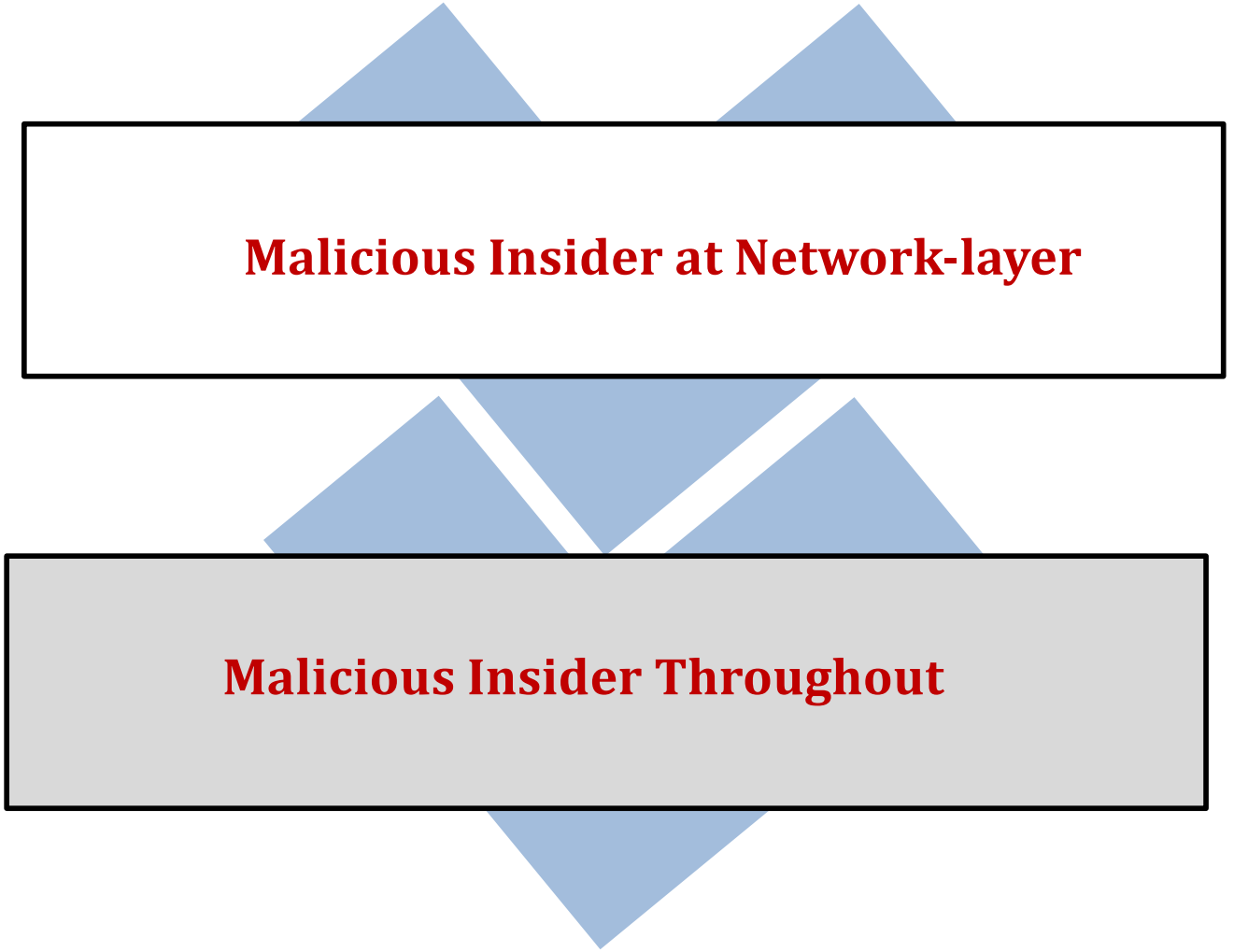
ATOM's Function permission list ∩ .Adoc policy

Question

What else could be missing in preventing the next insider threat?

Note: We will be referring to a few recent research work in this area by our group. Just to give you a glimpse of where the domain is headed to.

Advanced malicious insiders



--> novel, specific.

--> novel, most advanced.

Recent successful attack targeting homeland (Feb, 2019)

CNN World » Africa | Americas | Asia | Australia | China | Europe | Middle East | India | UK Live TV U.S. Edition +

Australian parliament's computer network targeted by unknown hacker

By Ben Westcott, CNN
Updated 10:56 PM ET, Thu February 7, 2019

Australia's Prime Minister Blames 'Sophisticated State Actor' for Parliament Hack

Prime Minister Scott Morrison of Australia making a statement on cyber security, on Monday.
Mick Tsikas/EPA, via Shutterstock

Attacks targeting internet's core network infrastructure

WikiLeaks Leaks News About Partners

Vault 7: CIA Hacking Tools Revealed

2

Cisco uncovers Telnet zero-day flaw in WikiLeaks' Vault 7 CIA dump

Users are advised to disable Telnet until a patch is available

3

CVE-2014-9295: ntpd buffer overflow vulnerability

Oct 1, 2018 · Advisory

4

Possible Backdoor Found in Chinese-Made Routers

Jill Scharr · Contributing Writer
Updated Aug 27, 2014

1

ars technica

MAIN MENU · MY STORIES: 25 · FORUMS SUBSCRIBE JOBS

LAW & DISORDER / CIVILIZATION & DISCONTE

Photos of an NSA "upgrade" factory show Cisco router getting implant

Servers, routers get "beacons" implanted at secret locations by NSA's TAO team.

by Sean Gallagher - May 15 2014, 4:30am +0900

HACKING NATIONAL SECURITY

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

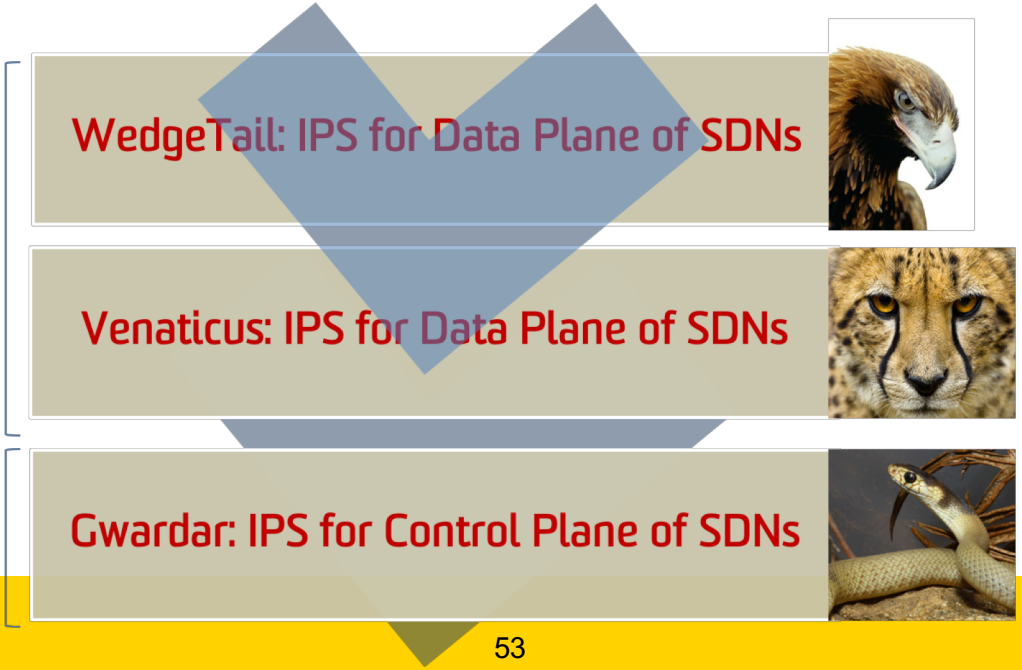
Insider Threat 5

Privileged IT users biggest risk to organizations (CA Threat Report 2018)

Malicious insider at Network-layer

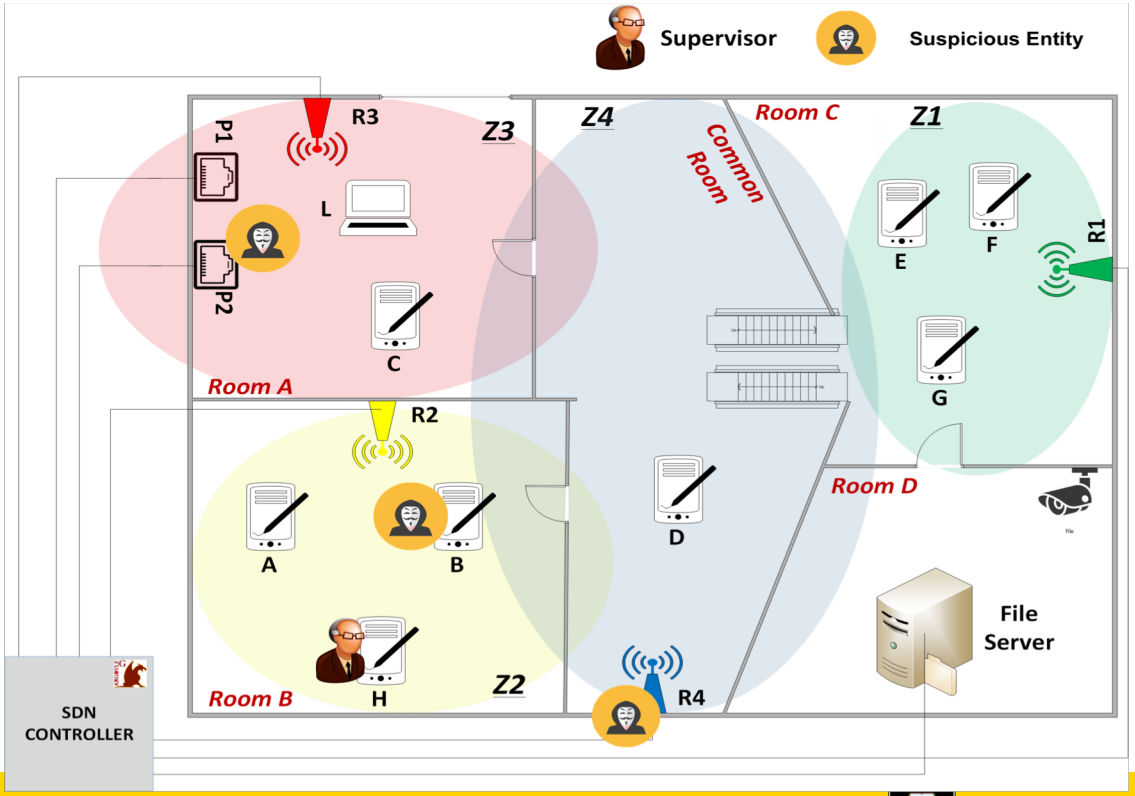
- Has access to network infrastructure
- Maliciously tampers with the network configurations
- Changes the packet forwarding setup throughout or for a subset of the network.

- We have proposed and developed early solutions to address this for Software-Defined Networks (SDNs) - the next generation of network architectures. If interested, see relevant papers.



Malicious Insider Throughout

- **“BYOD”**, “Anytime, Anywhere”
- Access both at application-layer and network-layer
- Assumed to exploit his access to compromise confidentiality, integrity, and availability (CIA) of the organization's data.



What's Missing?

1 **Fail to adapt to the '<u>negative changes</u>' in user's behaviour -- <u>even if it suggests attacking the system.</u>**

E.g. *hacking tools*

2 **Assuming that users follow the security rules.**

E.g. *An employee to access confidential information in a secure room over a secure connection and in the presence of a supervisor rather than having an access control system enforcing this policy.*

Existing CAC Solutions: What's Missing?

3 **Trusting the user's device integrated sensors for retrieving the context attributes.**

E.g. *GPS hack*

4 **A binary approach to access decisions. Context is not deterministic, so can not be access control.**

E.g. *A user accessing sensitive information in an `insecure context' must not share (e.g. Email) but can read (e.g., View)*

Existing CAC Solutions: What's Missing?

5 **Relying on single access enforcement point.**

E.g. *if an attacker compromises a mobile device, it can still be prevented from targeting the organization's services.*

Preventing Malicious Insider Throughout

- Several different solutions have recently proposed each addressing one or more of the aforementioned challenges. If interested, we have surveyed some below:
  - Shaghaghi, Arash, et al. "Gargoyle: A Network-based Insider Attack Resilient Framework for Organizations." *arXiv preprint arXiv:1807.02593* (2018).

GARGOYLE:
A Network-based Insider Attack Resilient Framework for Organizations

Shaghaghi, Arash, et al. "Gargoyle: A Network-based Insider Attack Resilient Framework for Organizations." *arXiv preprint arXiv:1807.02593* (2018).

Reading List

For Insider Threats:

- Insider Threats (Cornell Studies in Security Affairs)
  - https://www.amazon.com/Insider-Threats-Cornell-Studies-Security/dp/1501705172 (UNSW has online access)
- CA Insider Threat Report 2018.
  - **https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf** (public)
- Liu, Liu, et al. "Detecting and preventing cyber insider threats: a survey." *IEEE Communications Surveys & Tutorials* 20.2 (2018): 1397-1417. (UNSW library has access)
- Homoliak, Ivan, et al. "Insight into Insiders: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures." *arXiv preprint arXiv:1805.01612* (2018).

For Access Control:

- Computer Security: Art and Science, Matt Bishop
  - https://pearson.com.au/products/A-C-Bishop/A-C-Bishop-Matt/Computer-Security-Art-and-Science/9780321712332?R=9780321712332 (UNSW library has physical copies)

Reading List

For Access Control:

- Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." *Proceedings of the 13th ACM conference on Computer and communications security*. Acm, 2006.

Related published work in this area mentioned in the lecture:

- Desmedt, Yvo, and Arash Shaghaghi. "Function-Based Access Control (FBAC): Towards Preventing Insider Threats in Organizations." *From Database to Cyber Security*. Springer, Cham, 2018. 143-165.
- Desmedt, Yvo, and Arash Shaghaghi. "Function-Based Access Control (FBAC): from access control matrix to access control tensor." *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*. ACM, 2016.

- Shaghaghi, Arash, Mohamed Ali Kaafar, and Sanjay Jha. "Wedgetail: An intrusion prevention system for the data plane of software defined networks." *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. ACM, 2017.
- Shaghaghi, Arash, et al. "Gwardar: Towards Protecting a Software-Defined Network from Malicious Network Operating Systems." *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*. IEEE, 2018.
- Shaghaghi, Arash, et al. "Gargoyle: A Network-based Insider Attack Resilient Framework for Organizations." *arXiv preprint arXiv:1807.02593* (2018).