Security in Distributed Computing

Von Welch

June 22, 2011

CENTER FOR APPLIED CYBERSECURITY RESEARCH

INDIANA UNIVERSITY

Pervasive Technology Institute

Overview of talk

First Hour:

What is cybersecurity?

How to think like a cybersecurity person:

- Attacks
- Defenses

Second Hour:

OSG and Cybersecurity: Mapping the first hour onto the OSG.

What is cybersecurity?

“The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users." https://secure.wikimedia.org/wikipedia/en/wiki / Cybersecurity

"Security is the process of maintaining an acceptable level of perceived risk." - Richard Bejtlick

"measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" http://www.merriam-webster.com/dictionary /cybersecurity

My version...

The art and science of maintaining an acceptable level of perceived risk under threat of attacks by malicious parties.

Cybersecurity uses a number of tools

Training and policy

Identity Management

Cryptography

Limited Privilege

Monitoring and Auditing

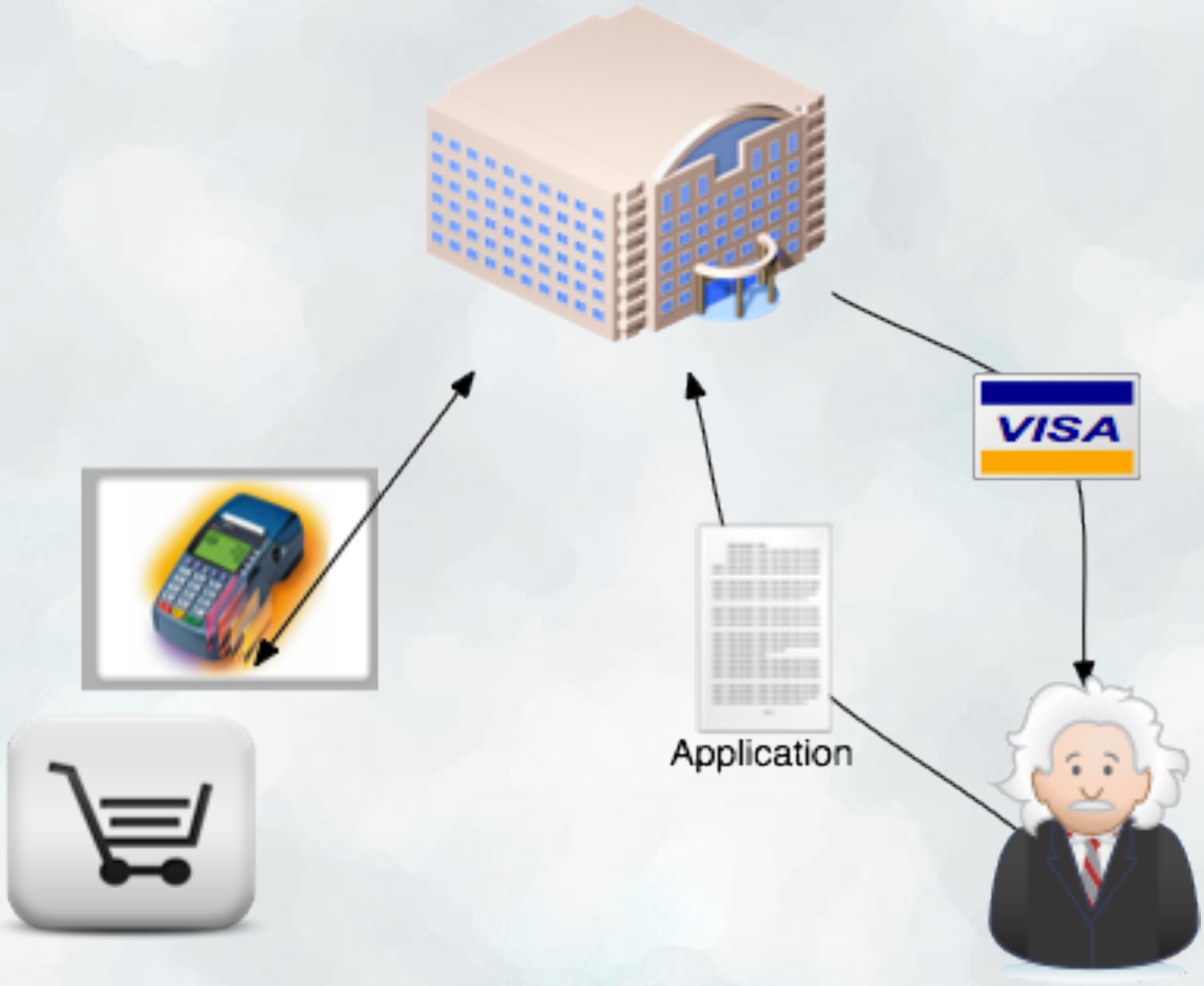
Revocation

More on these later...

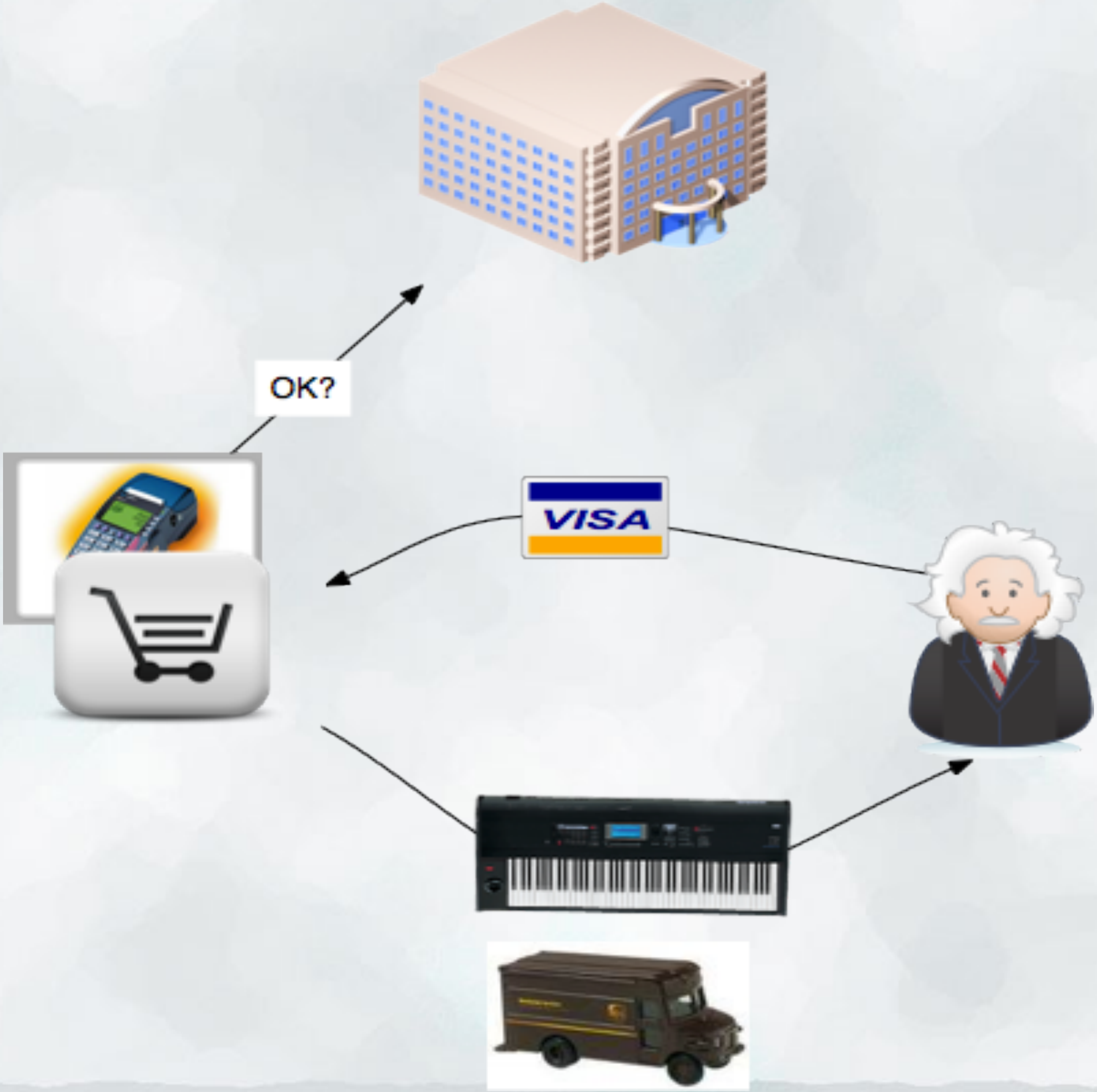
Let's take a simple scenario...

Online credit card purchase.

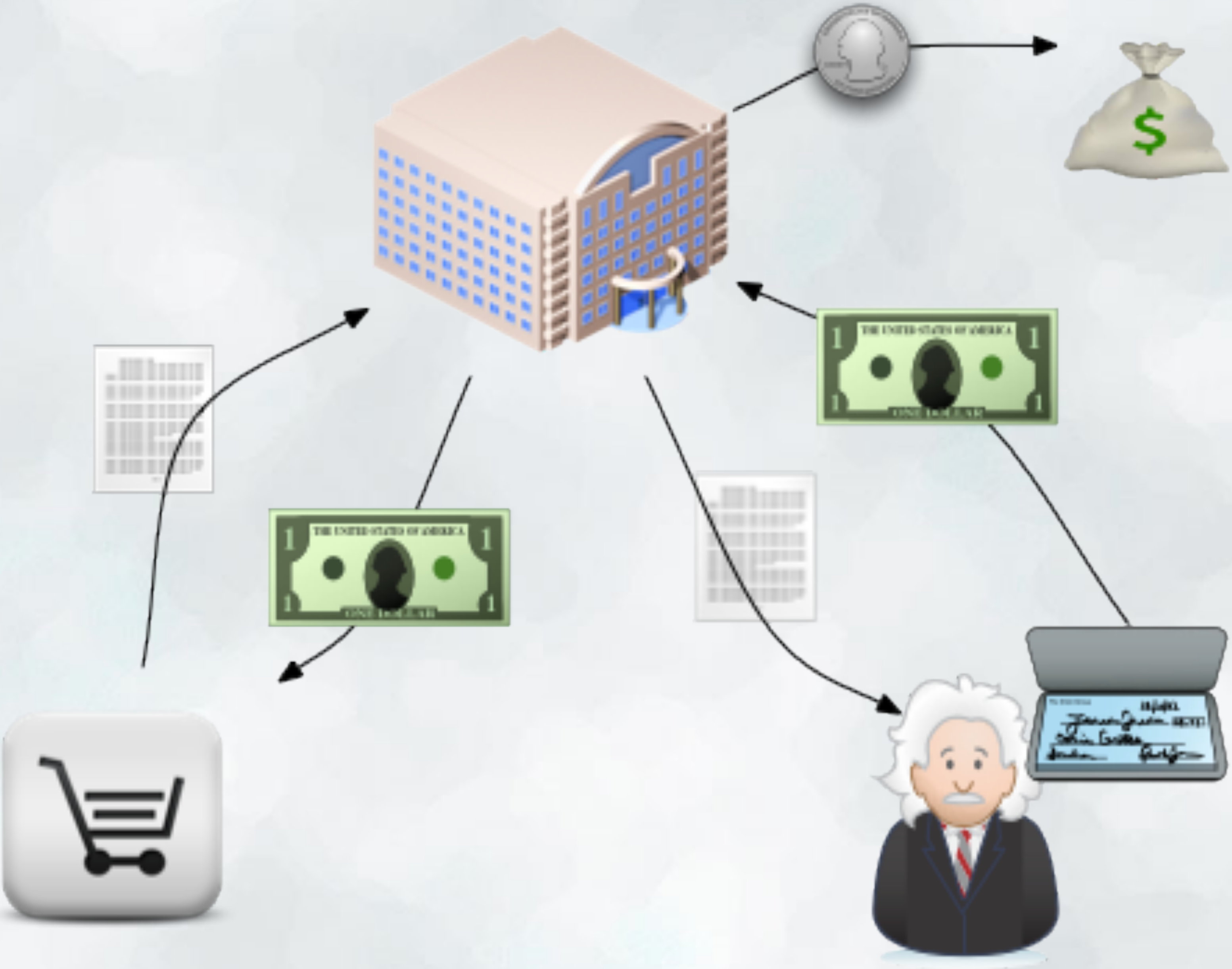
Registration



Purchase



Reconciliation



How do we go about securing credit card transactions?

First step, what is it we are securing?

Assets

Things of value.

May be tangible or intangible.

Are often the goals of attack.

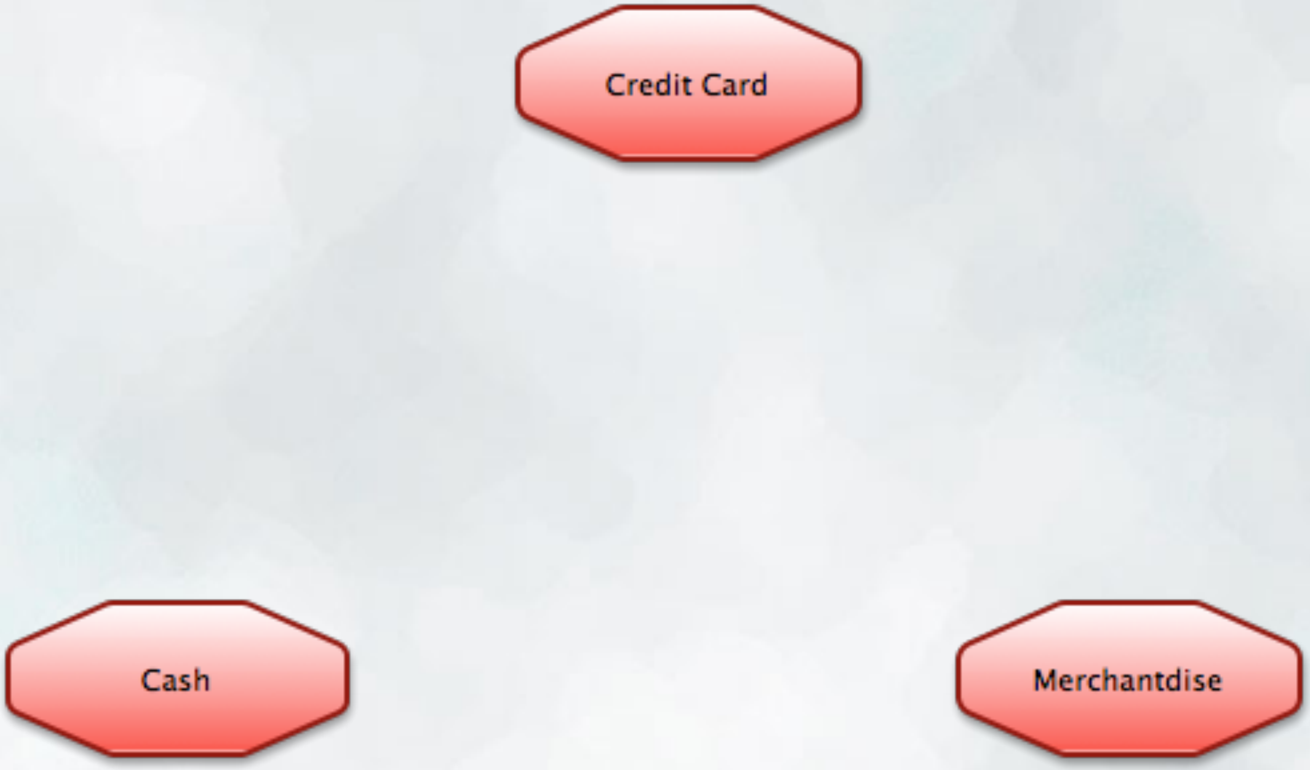
Assets

What are the assets in the credit card scenario?

Some assets in credit card scenario...

- Money
- Merchandise
- Credit Card

Building an Attack diagram



Credit Card

Cash

Merchantdise

How would we go about attacking?

First step to figuring out how to defend

Some types of attack...

Impersonation

Stealing confidential information/eavesdropping

Tampering with data/messages

Compromising an entity

Fraud (lying)

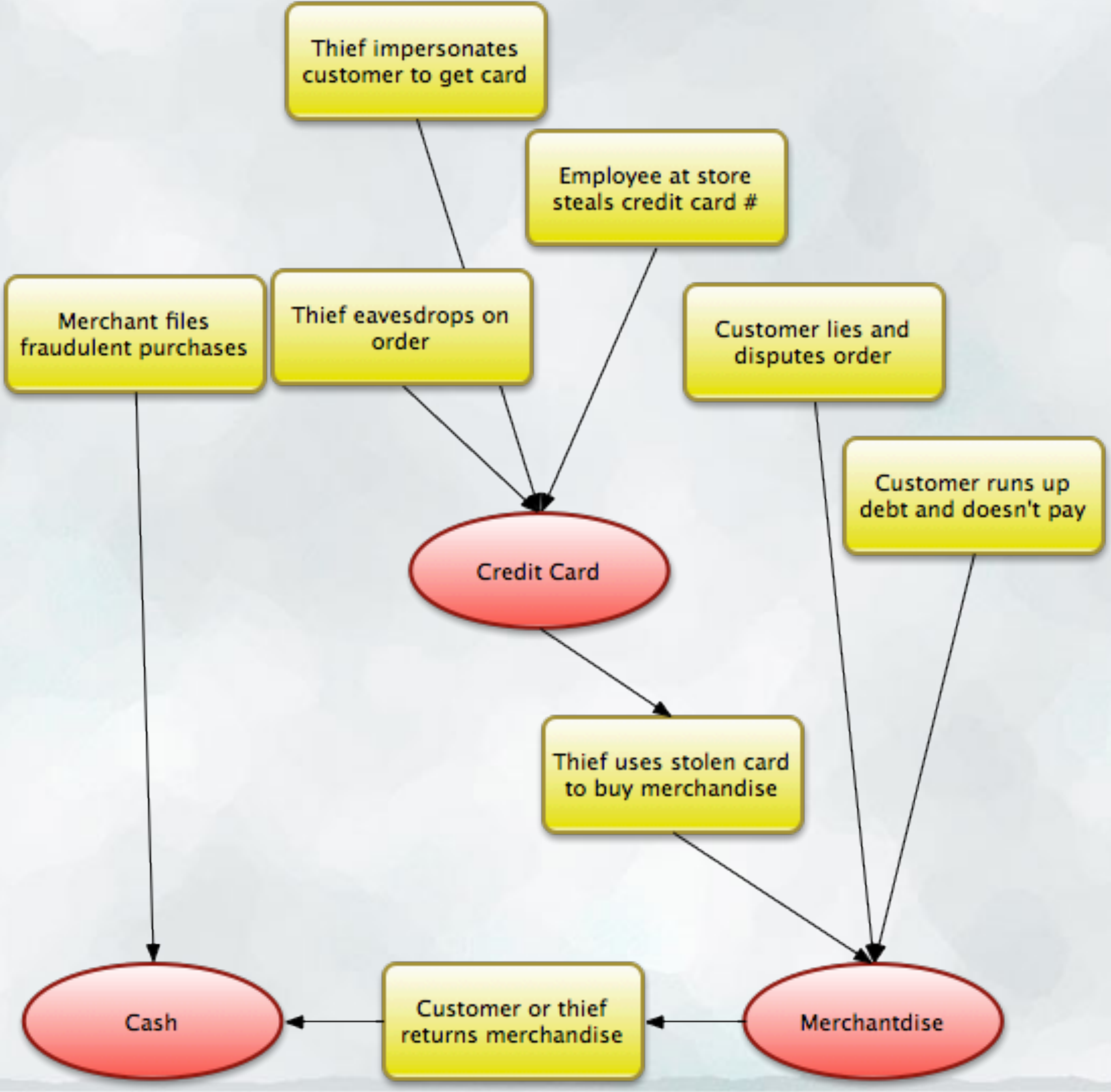
Abusing trust

How would you attack the credit card scenario?

Some attack ideas...

Impersonate a customer to get a card.
Run up a bunch of debt and don't pay.
Eavesdrop on the connection and steal card #.
Tamper with order and change ship-to address.
Merchant lies to the bank about a sale.
Employee at merchant steals card #s
Customer lies to the bank about a sale not taking place.
Hacker compromises customer computer and buys stuff.
And many more...

Attack Diagram


Thief impersonates customer to get card
Employee at store steals credit card #
Merchant files fraudulent purchases
Thief eavesdrops on order
Customer lies and disputes order
Customer runs up debt and doesn't pay
Credit Card
Thief uses stolen card to buy merchandise
Cash
Customer or thief returns merchandise
Merchantdise

Now let's turn to defending...

But first, let's consider our constraints....

Constraints...

Cost

Performance

Usability

Level of trust in participants

Dealing with Failure

Cost

What is the asset we're guarding worth?

How much will it cost if it is compromised?

How much loss is tolerable?

Performance

How much time can security take?

How much can we slow down the different processes?

Usability

How tolerant are all the participants of extra effort?

How much training do they have?

How often do they need to use the system?

Trust level

We expect all the participants to behave appropriately.

How much do we trust them to do so?

What happens if security breaks?

If our security breaks what happens?

Can we fall back to less secure methods?

How much failure can we afford? Retries OK?

Let's talk defense...

Set of processes for preventing, detecting, and responding to attacks.

For each attack...

Consider how it will be:

Prevented

Detected

Responded to

Defense tools

Training and policy

Identity Management

Cryptography

Limited Privilege

Monitoring and Auditing

Revocation

Training and policy

All participants have roles that they play - procedures they follow (and things they avoid doing).

Some is enforced by technology.

Much is enforced because of policy and training.

What training do all the participants in the credit card scenario have?

Training and policy

Examples...

Customers trained to keep CC# secret

Stores don't allow merchandise bought with
CC to be returned for cash.

Merchants must check with bank during purchase.

Identity Management

Vetting and enrolling users

Establishing an authentication mechanism (passwords, certificate, etc.)

Establishing privileges

Conveying that information to services

Compromised identities - Revocation

Cryptography

Protecting data via:

Confidentiality (secrecy)

Integrity (protection from tampering)

Authentication (who is it from)

Limiting Privilege

Limiting trust in participants.

Preventing abuse.

Limiting fallout if something bad happens.

May cause usability problems if limits are hit often.

Monitoring and Auditing

Watching what is happening.
Keeping records of what is happening.
Reviewing those records

Detecting suspicious events in real time.

Following up later and making sure what happened is what should have happened.
(Policy was followed.)

Revocation

Taking away a privilege you gave out.

Can be difficult...

Take credential back.

Or have to tell everyone credential is no good.

Applying defenses to our credit card scenario...

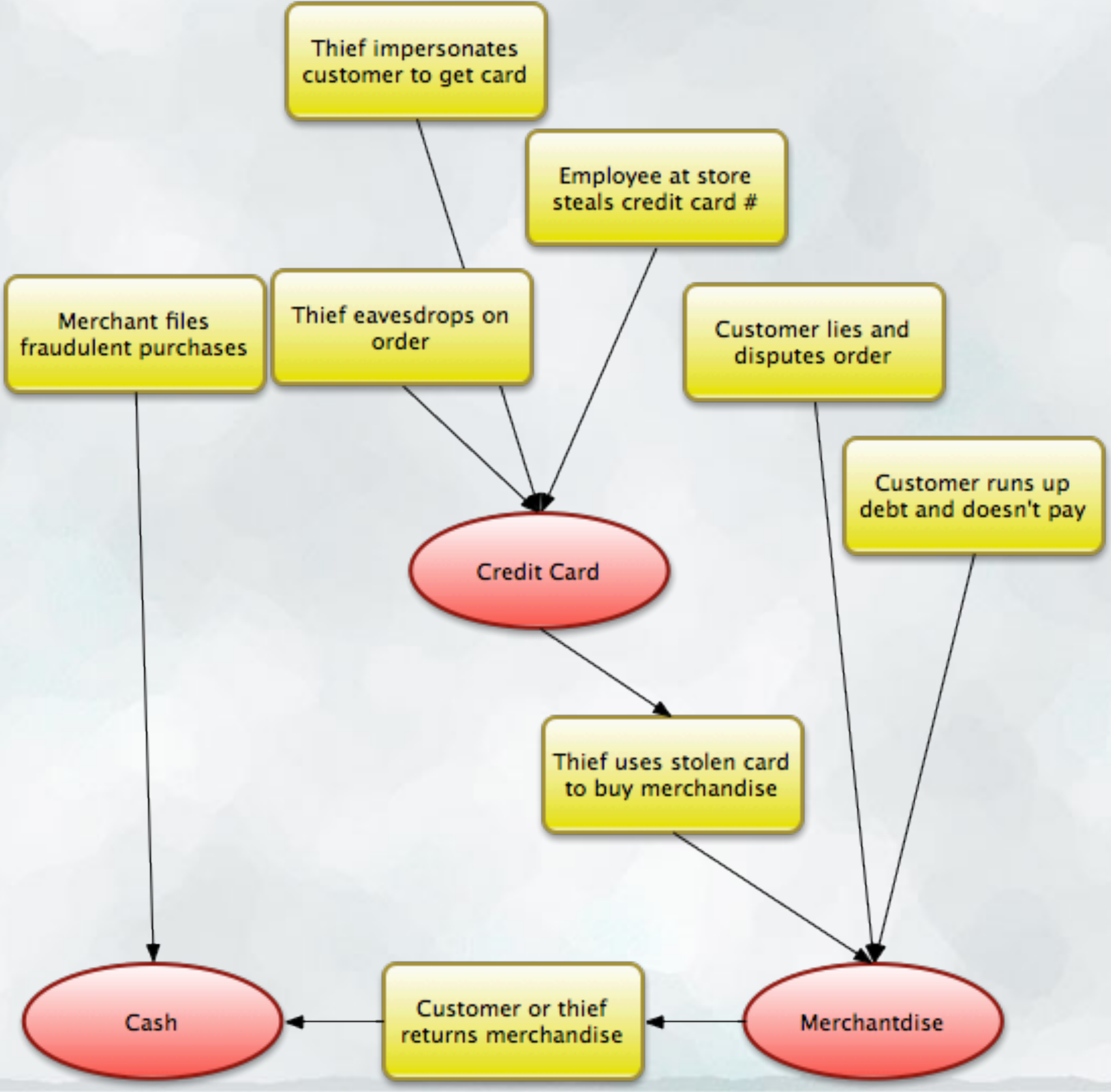
You can't prevent all the attacks all of the time.

Try to prevent most,
detect all.

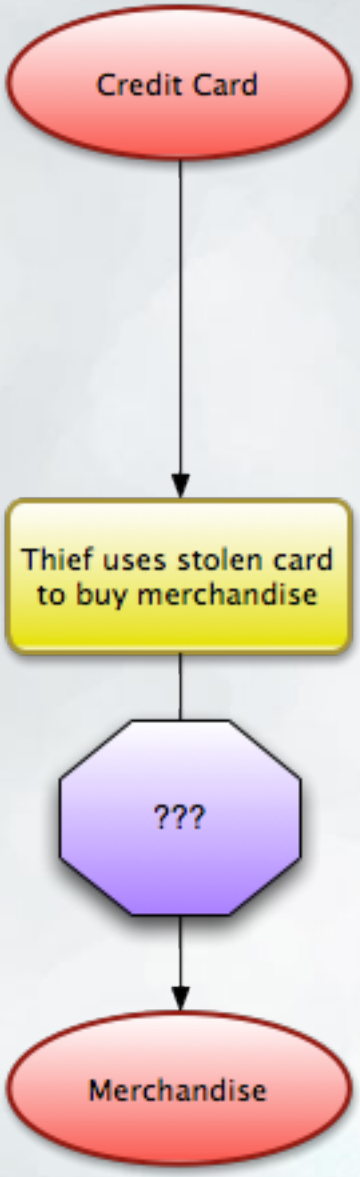
Applying defenses to our credit card scenario...

What defenses can you name?

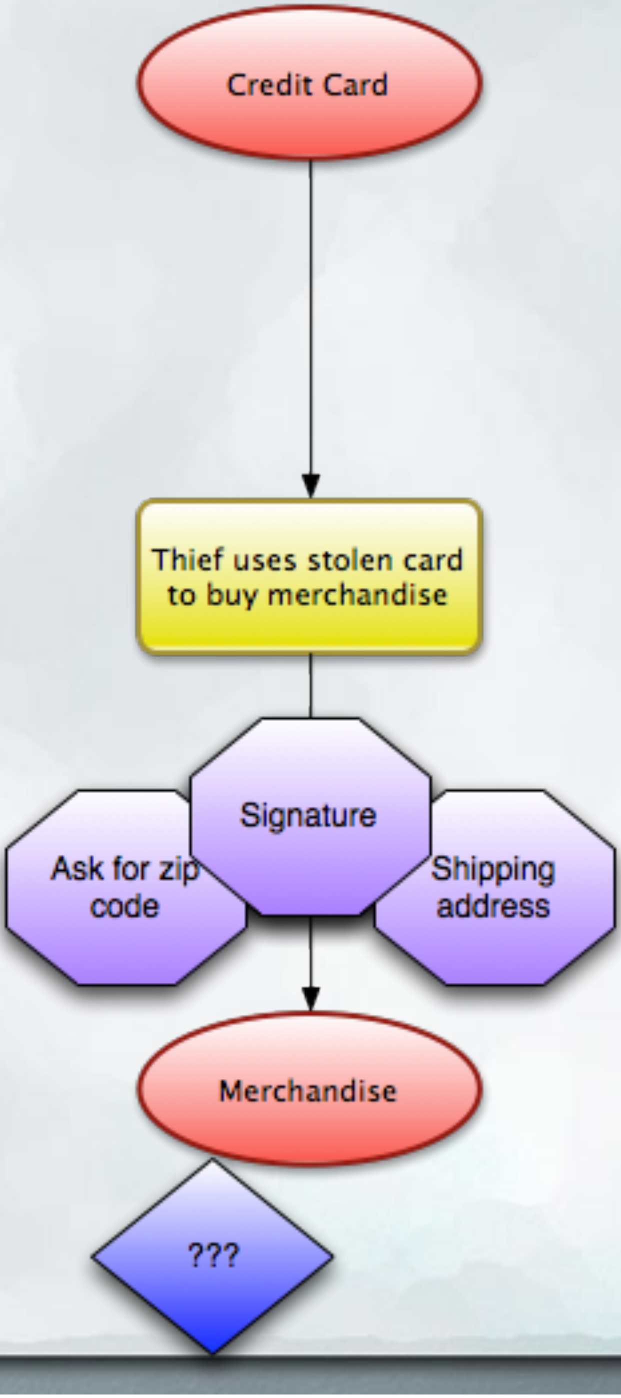
Attack Diagram


Thief impersonates customer to get card
Employee at store steals credit card #
Merchant files fraudulent purchases
Thief eavesdrops on order
Customer lies and disputes order
Customer runs up debt and doesn't pay
Credit Card
Thief uses stolen card to buy merchandise
Cash
Customer or thief returns merchandise
Merchantdise

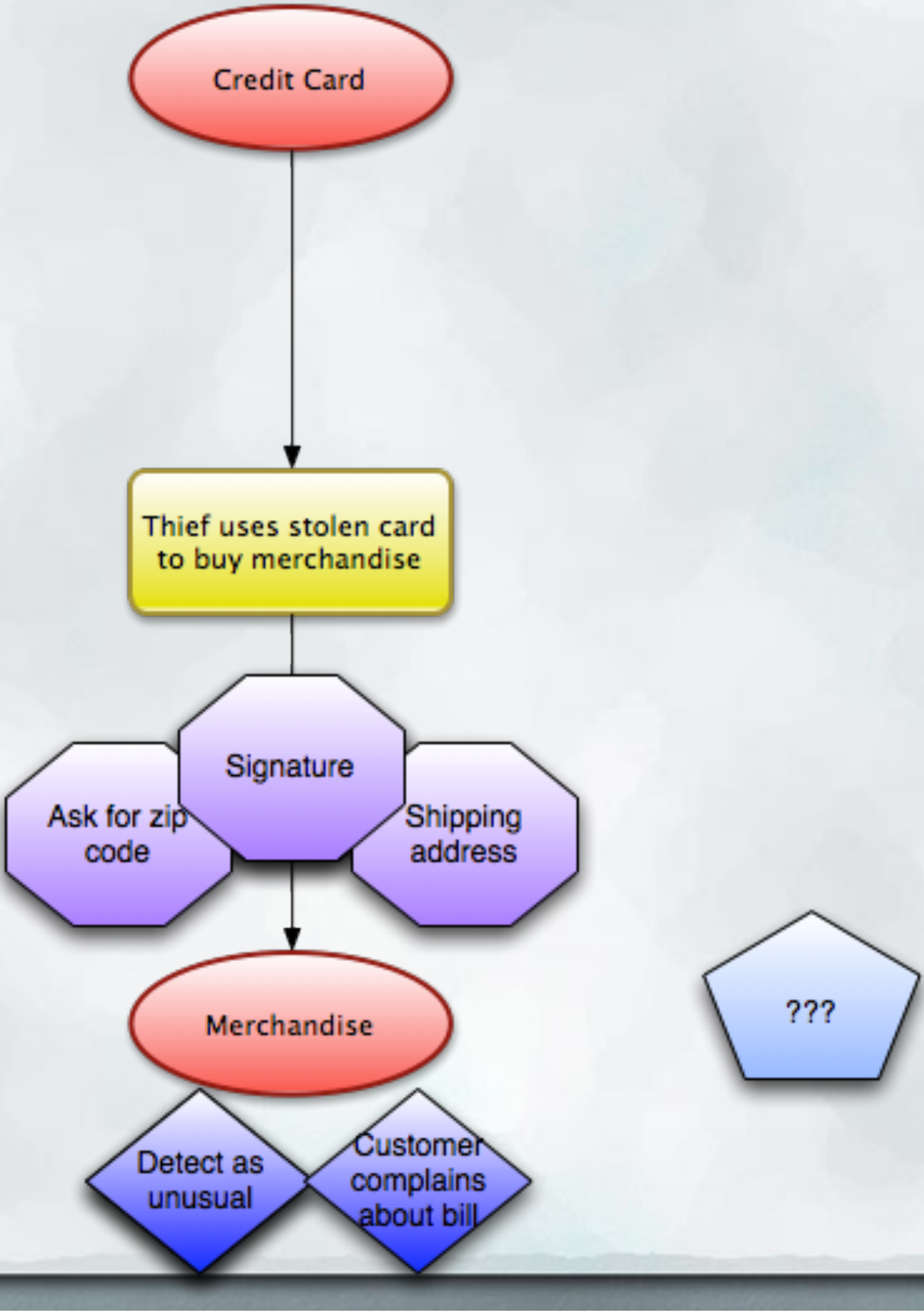
Focusing in on an attack...



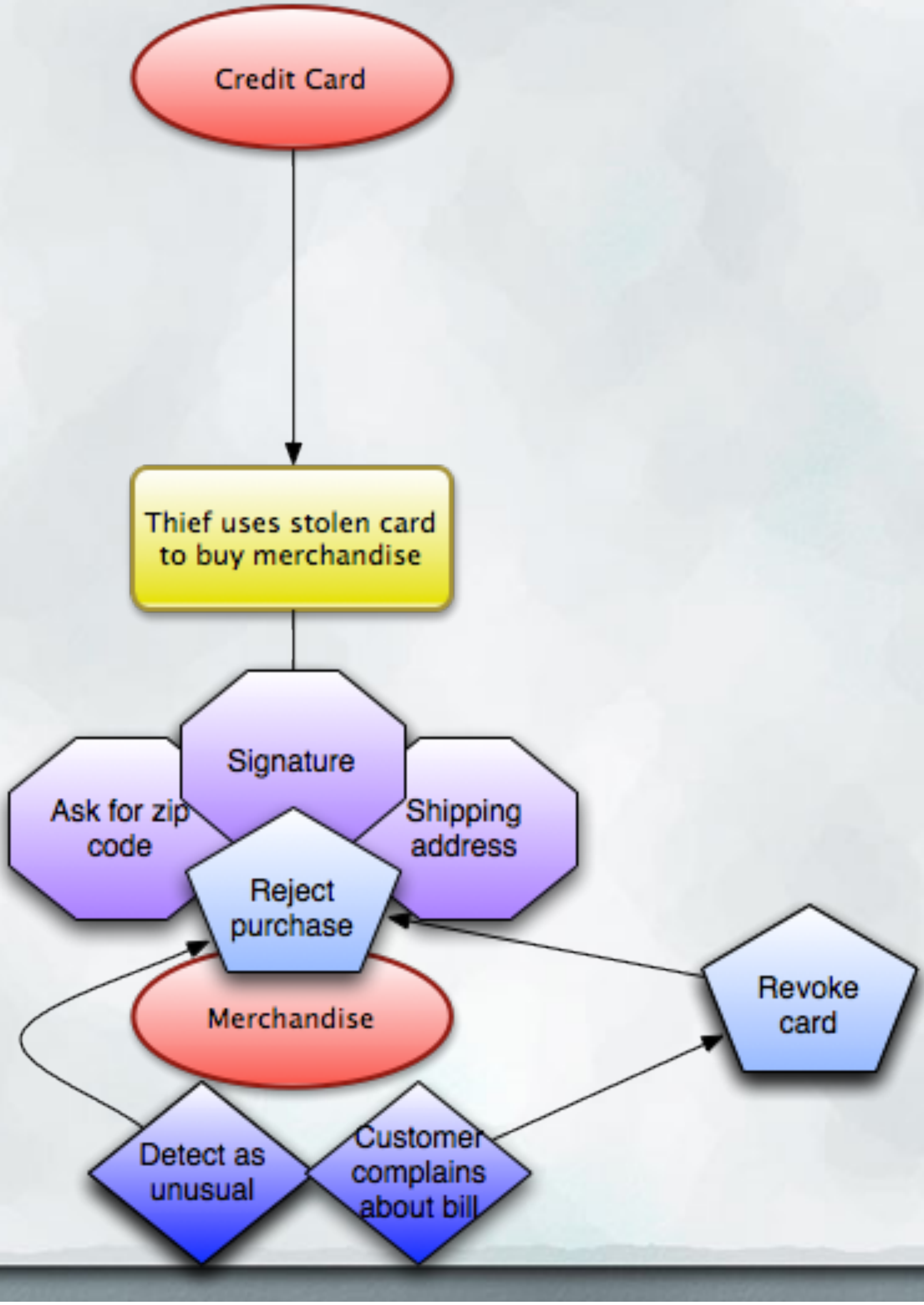
Prevention


Credit Card
Thief uses stolen card to buy merchandise
Signature
Ask for zip code
Shipping address
Merchandise
???

Detection


Credit Card
Thief uses stolen card to buy merchandise
Signature
Ask for zip code
Shipping address
Merchandise
???
Detect as unusual
Customer complains about bill

Response


Credit Card
Thief uses stolen card to buy merchandise
Signature
Ask for zip code
Shipping address
Reject purchase
Merchandise
Revoke card
Detect as unusual
Customer complains about bill

Summary of process

Determine what you are defending

Determine how it could be attacked

Determine what your limitations are for defending it

Apply defenses:
prevention, detection, response.

Break

Cybersecurity and OSG

Let's apply the cybersecurity concepts to OSG...

Let's start with assets again...

But first, let's talk about "secondary assets"

Secondary assets

Something that isn't valuable in itself, but is a significant step to obtaining something valuable.

For example, car keys aren't that valuable unto themselves, ‘but they make getting a car much easier.

What OSG Assets can you name?

Some OSG Assets

Compute elements

Science data

Storage elements

OSG Secondary Assets

User credentials

VOMS membership database

Software stack

OSG Assets

Compute Elements

Storage Elements

Science Data

Some types of attack (review)

Impersonation

Stealing confidential information/eavesdropping

Tampering with data/messages

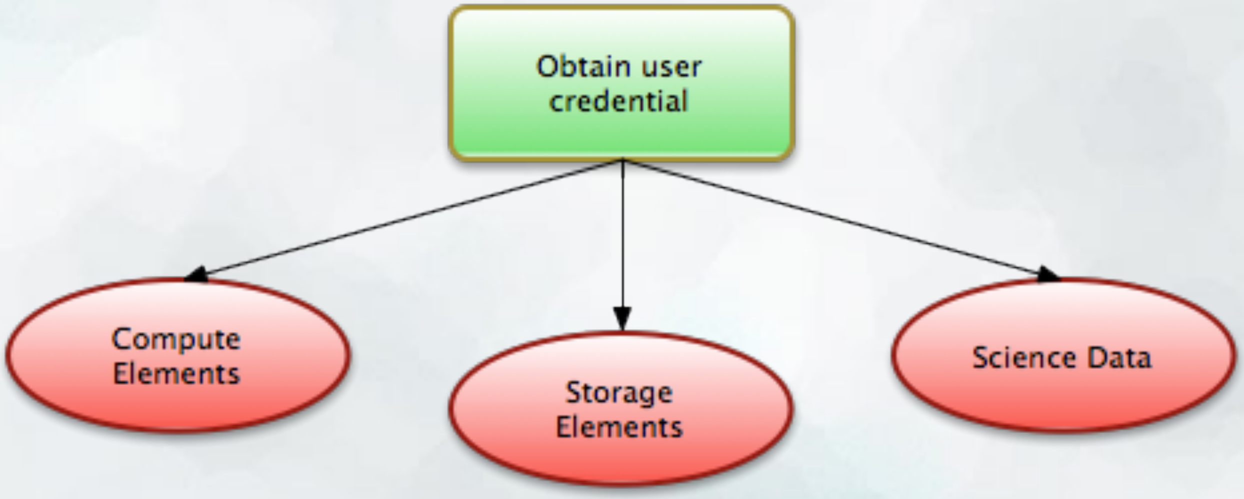
Compromising an entity

Fraud (lying)

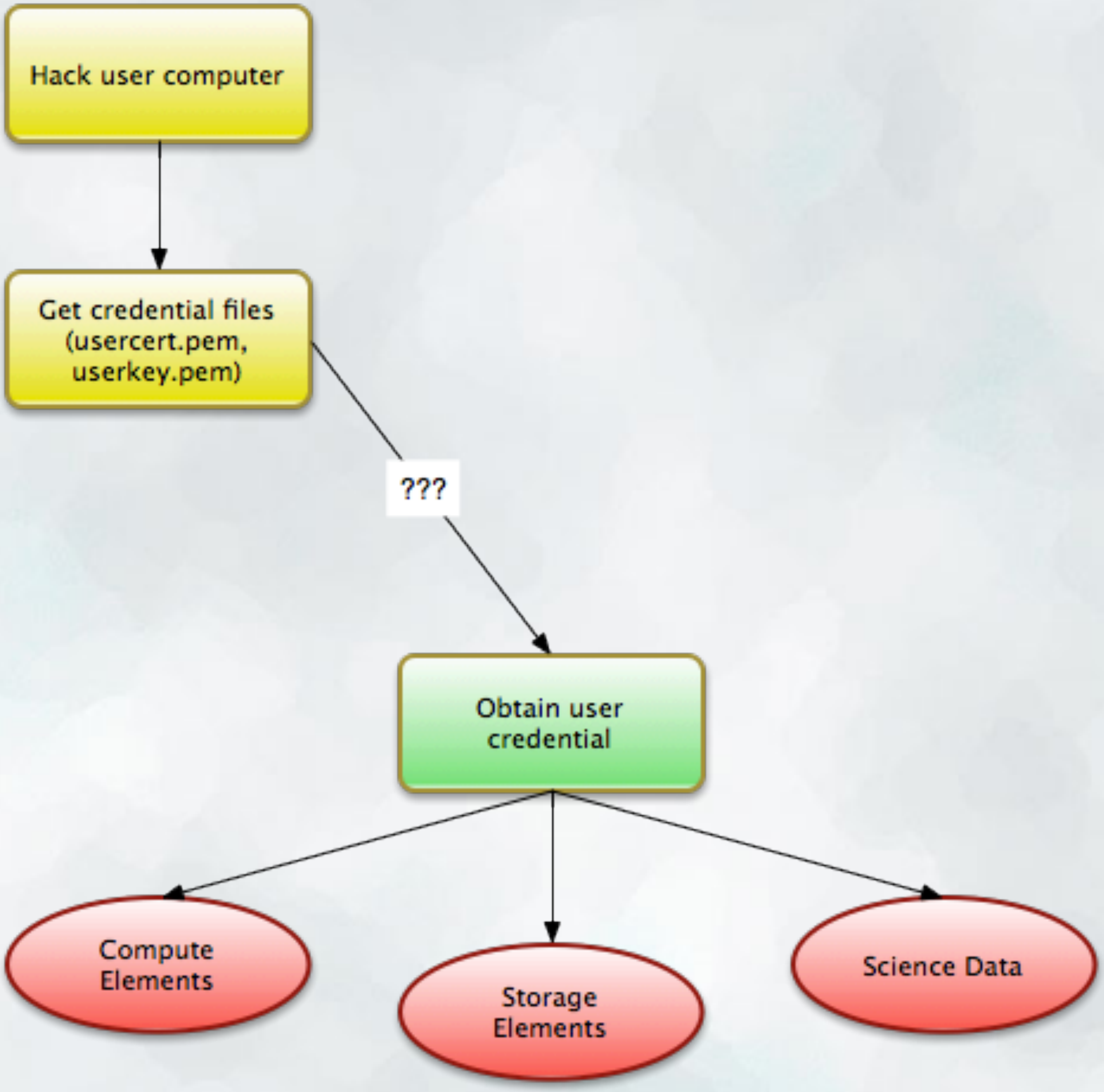
Abusing trust

How would you go about attacking the OSG?

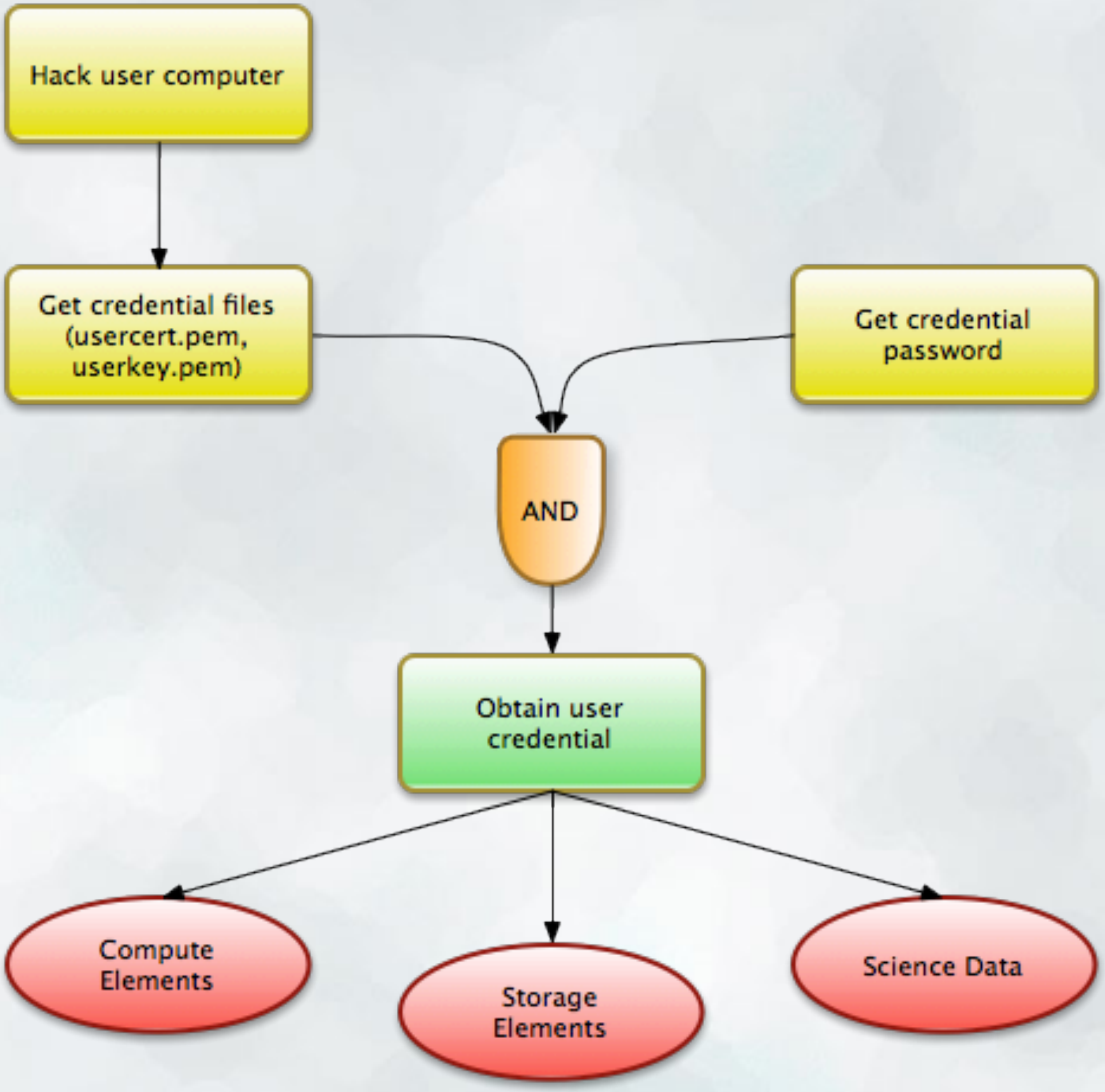
An example OSG attack



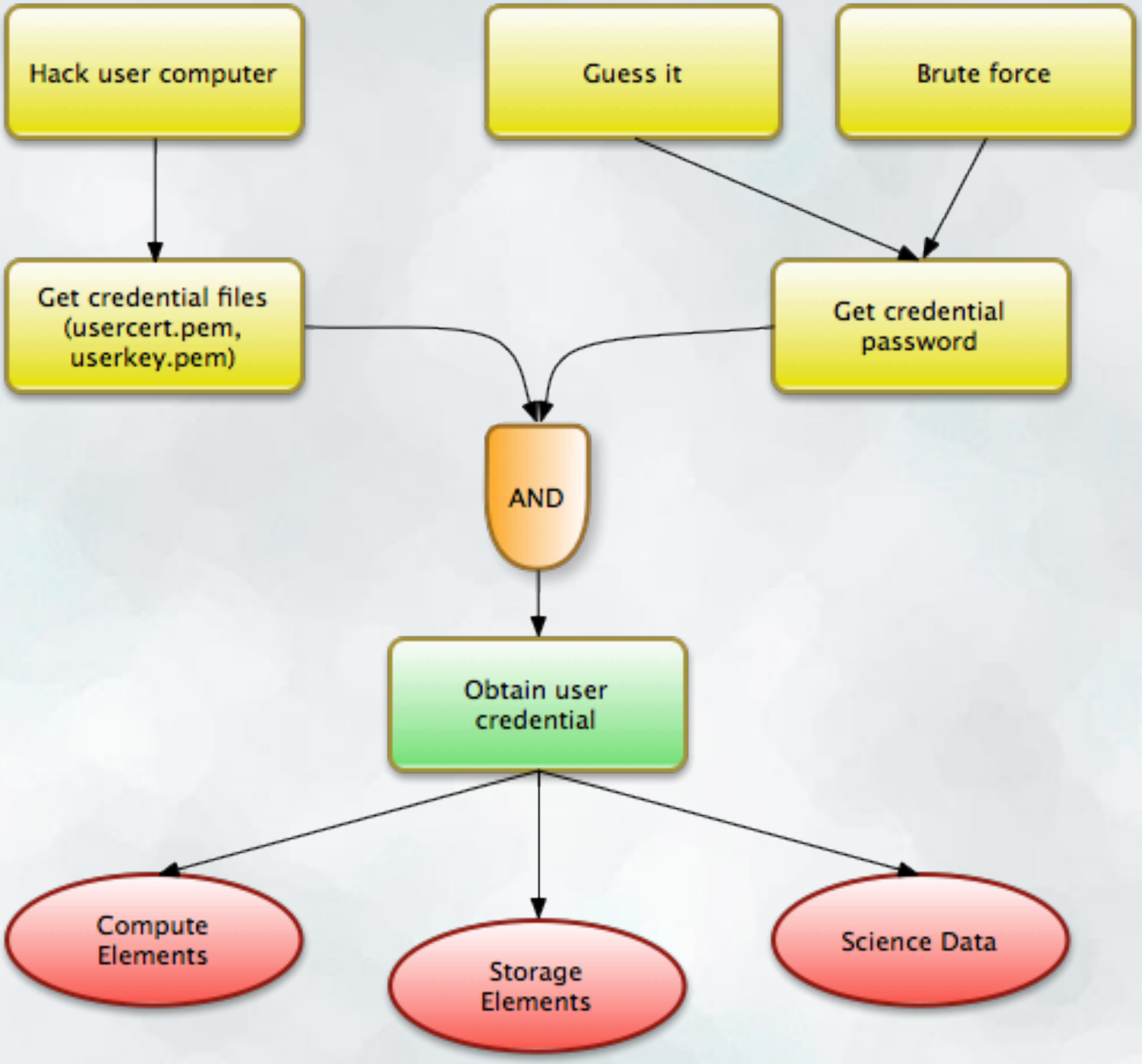
An example OSG attack



An example OSG attack



An example OSG attack



Defending the OSG

As before, let's review our constraints.

Cost

What is the asset that we're guarding worth?

How much will it cost if it is compromised?

How much loss is tolerable?

Performance

How much time can security take?

Usability

How tolerant are all the participants of extra effort?

How much training do they have?

How often do they need to use the system?

Trust level

We expect all the participants to behave appropriately.

How much do we trust them to do so?

What happens if security breaks?

If our security breaks what happens?

Does the system break?

Do we fall back to less secure methods?

How much failure can we afford?

Defense tools

Training and policy

Identity Management

Cryptography

Limited Privilege

Monitoring and Auditing

Revocation

Training and policy

All participants have roles that they play - procedures they follow (and things they avoid doing).

Some is enforced by technology.

Much is enforced because of policy and training.

OSG examples?

Training and policy

Acceptable use policy

Password protecting credentials

Keeping systems patched

Summer schools

Training for sites

etc.

Identity Management

Vetting and enrolling users

Establishing an authentication mechanism (passwords, certificate, etc.)

Establishing privileges

Conveying that information to services

Compromised identities - Revocation

Identity Management

PKI for authentication

with Proxy Certificate for single sign-on
(voms-proxy-init)

VOMS for virtual organization support

PRIMA/GUMS for service-side authorization

Cryptography

Protecting data via:

Confidentiality (secrecy)

Integrity (protection from tampering)

Authentication (who is it from)

Cryptography

Used in SSL to encrypt communications (job submission, data transfer, etc.)

Used in identity management for certificates, proxy certificates, securing VOMS data.

Limiting Privilege

Limiting trust in participants.

Preventing abuse.

Limiting fallout if something bad happens.

May cause usability problems if limits are hit often.

Limited Privilege

Authorization based on membership

Processes run in unix accounts

Quotas on computation and storage

Monitoring and Auditing

Watching what is happening.
Keeping records of what is happening.

Detecting suspicious events in real time.

Following up later and making sure what happened is
what should have happened.
(Policy was followed.)

Monitoring and Auditing

Per-job auditing records via Gratia

VDT includes syslog-ng for centralized logging

Sites have their own IDS mechanisms

Revocation

Taking away a privilege you gave out

Can be difficult...

Take credential back

Or have to tell everyone credential is no good

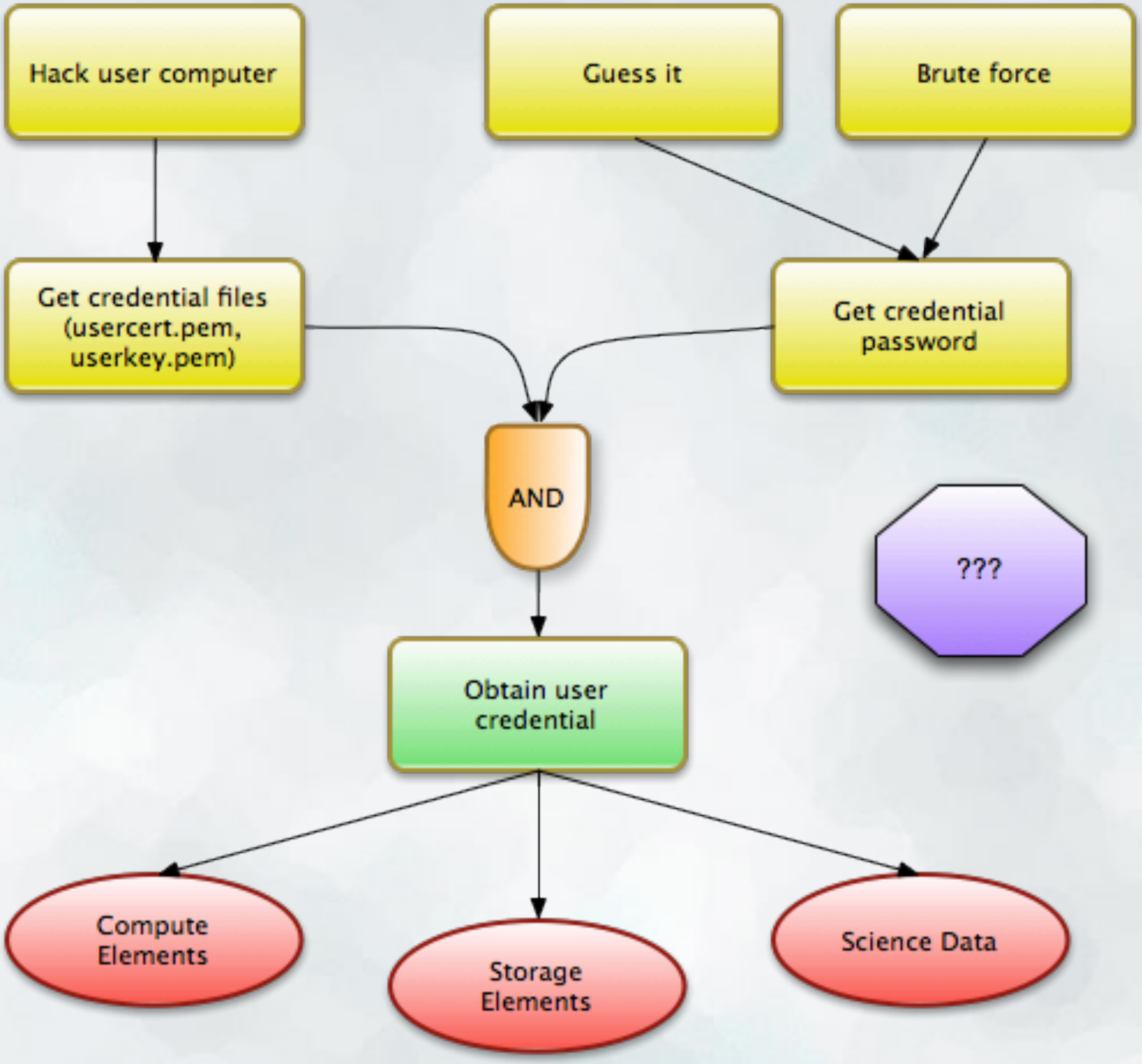
Revocation

PKI revocation is done by CAs

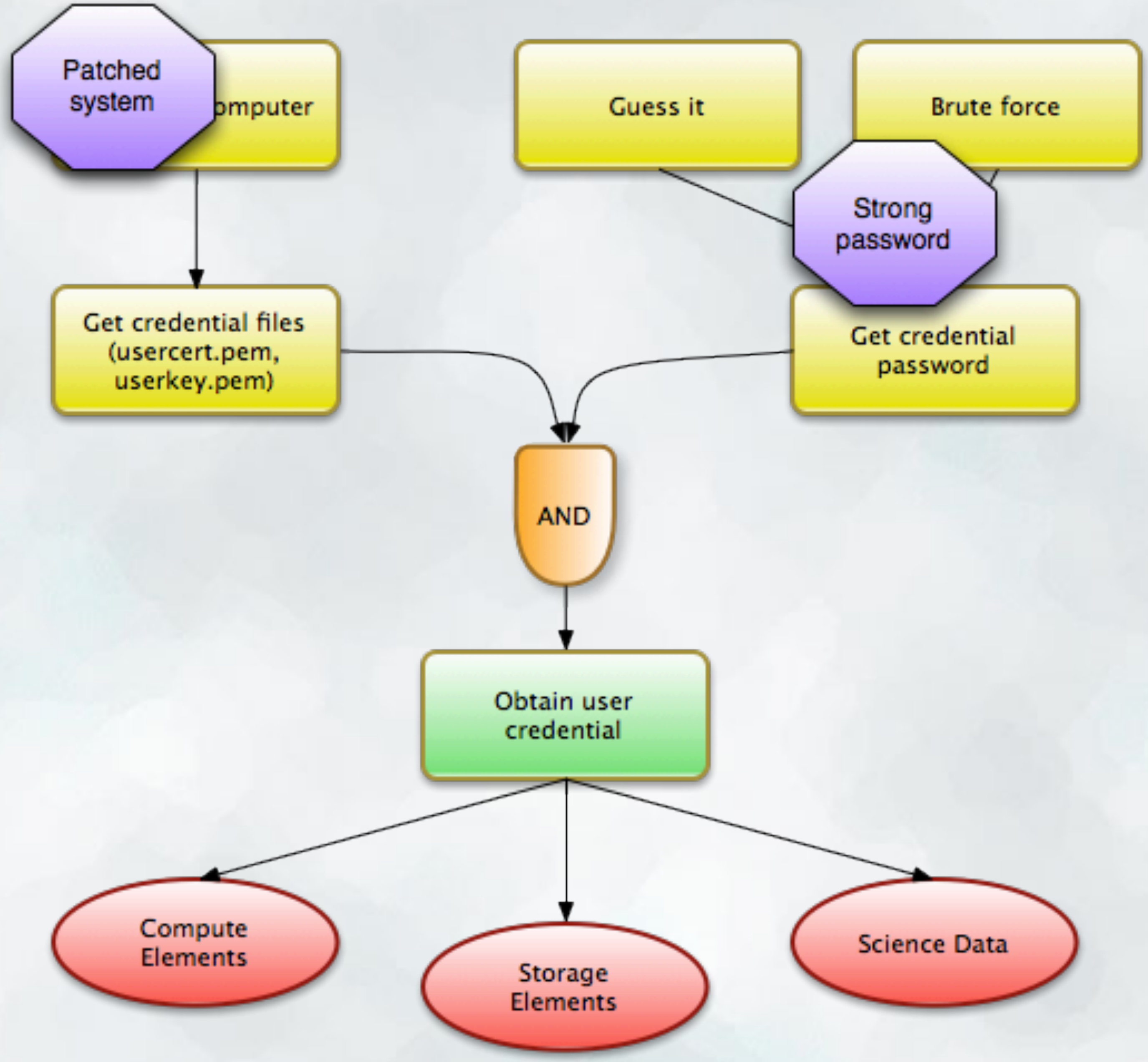
Distributed as a certificate revocation list (CRL)

Resources must pull down CRL frequently
and check certificates against it.

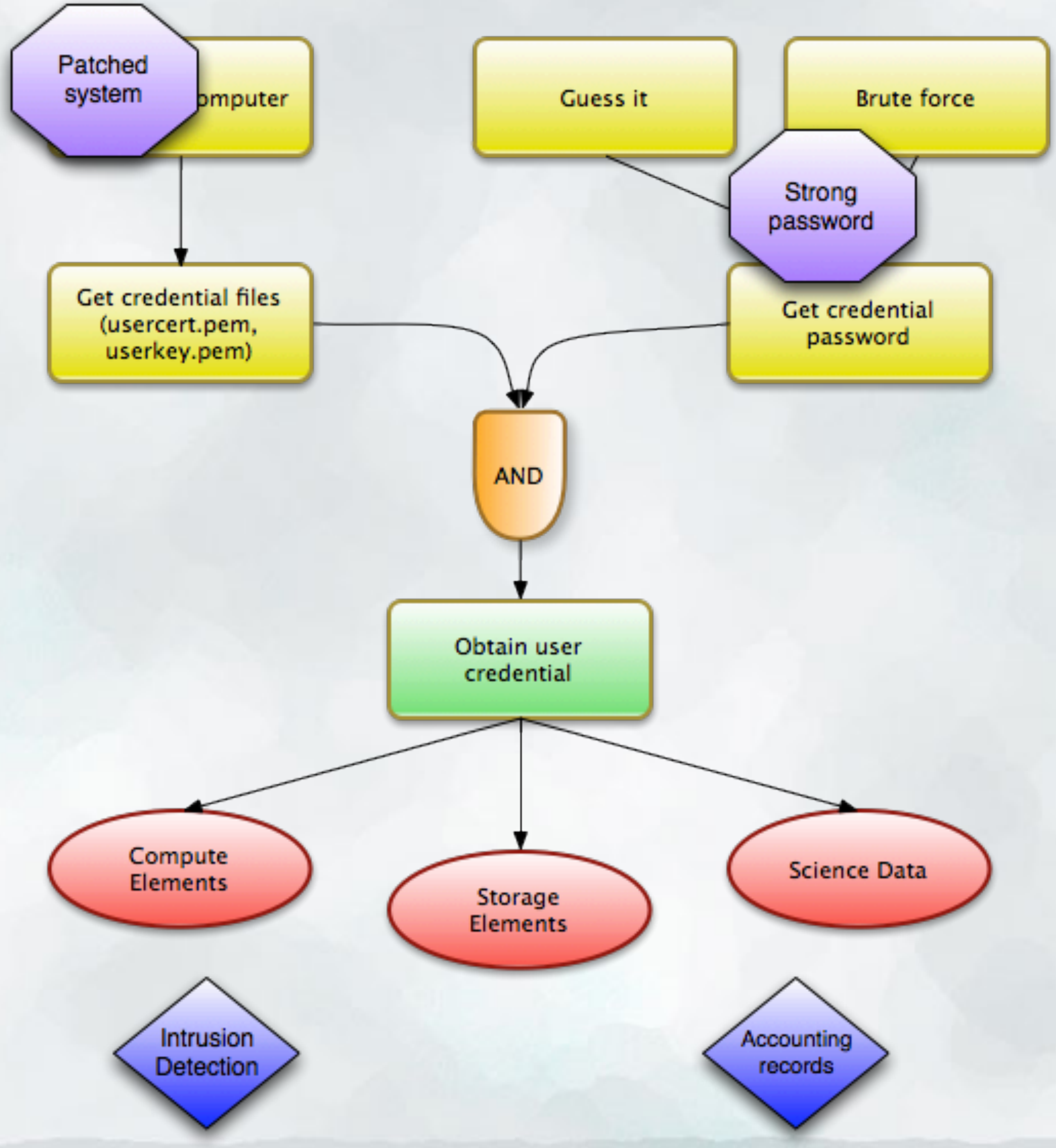
An example OSG attack



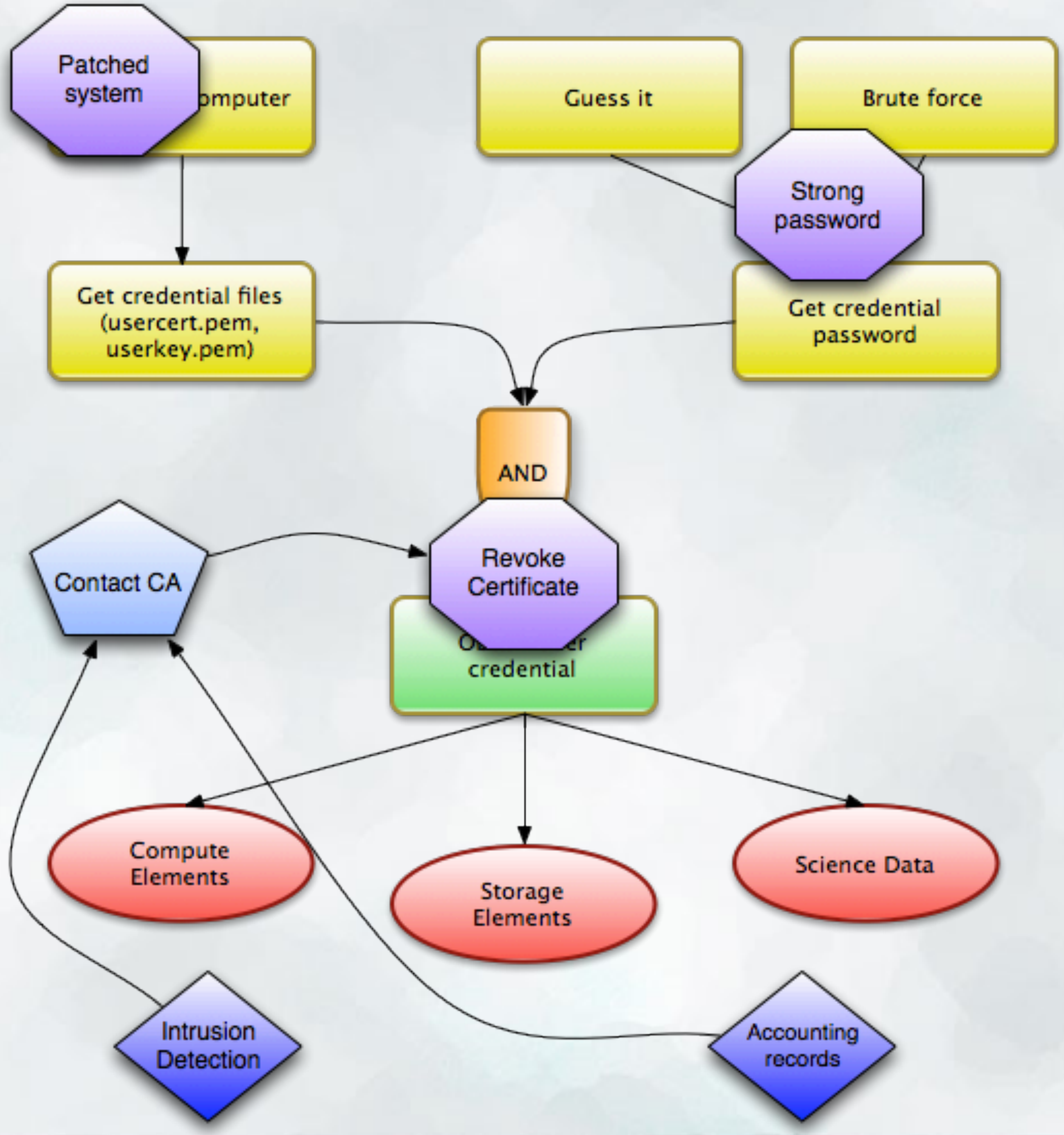
An example OSG attack



An example OSG attack



An example OSG attack



Summary of process

Discussed a process for planning cybersecurity defenses based on assets, attacks and constraints

Discussed categories of defenses

Discussed how OSG is defended based on those categories

Some extra thoughts....

Where are the incentives?

Who pays for security? Who suffers the loses?
What if they don't line up?

What if the damage to your infrastructure is largely
born by someone else?

Classic example: nuclear plant next to large city

Policy and law may be needed

Attackers have different motivations...

Some are after what is valuable to you and me

Some are joy riding

Proving your security is too weak

Activism

Hoping to get elsewhere through you

The world changes...

Security needs to be re-evaluated on a regular basis

For example:
Price of copper goes up, it becomes an interesting asset

Mechanisms weaken over time

Motivations of attackers change

Never assume you thought of every attack...

Get multiple sets of eyes to review

Even then assume you've missed something

Insider threat is particularly hard

Audit, audit, audit...

Some uncovered issues...

Privacy

The feeling of safety

Vulnerabilities/coding errors

Ethics, responsible disclosure

Thank you.

Acknowledgements

Thanks to Mine Altunay and Jim Basney for input on this presentation.

Cheryl Bennet, Dara Eckart, Kristy Kallback-Rose, Ryan Hartman, Suresh Marru, George Turner, Jim Williams for feedback on early version of this presentation.

vwelch@indiana.edu

CENTER FOR APPLIED
CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute