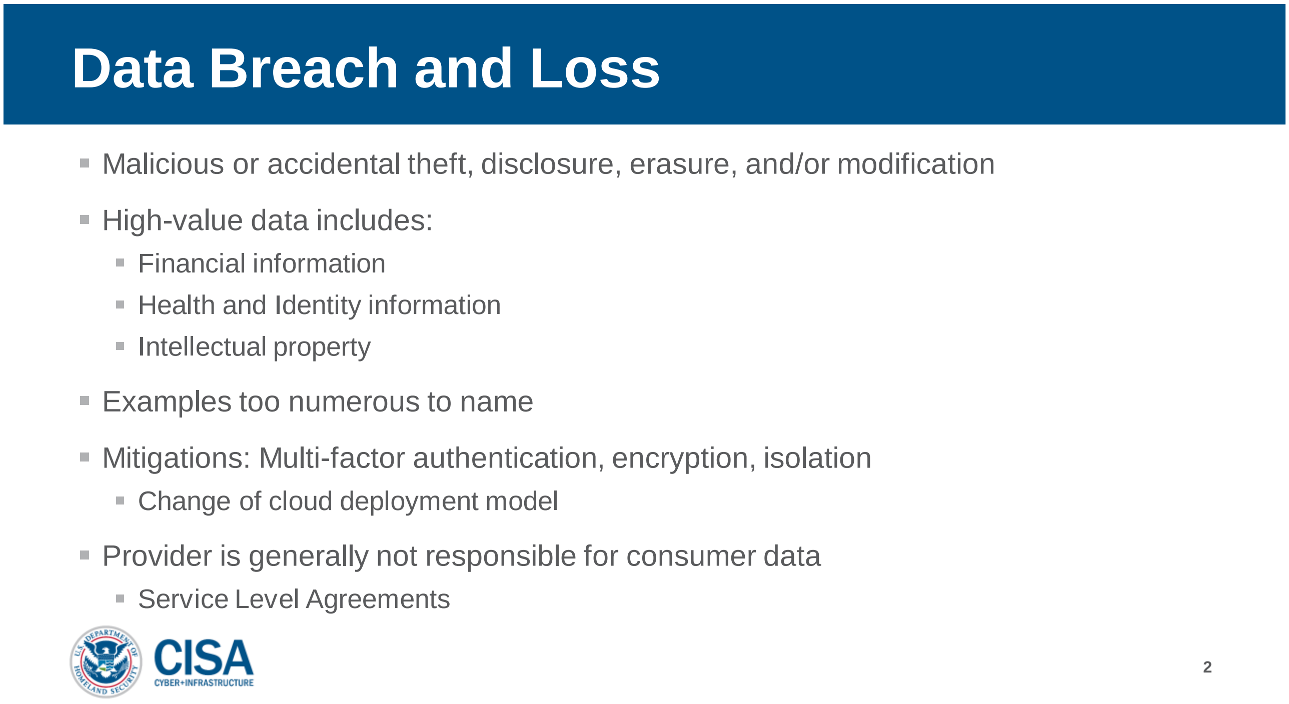
Cloud Threats and Attacks

Table of Contents

Data Breach and Loss



Data Breach and Loss

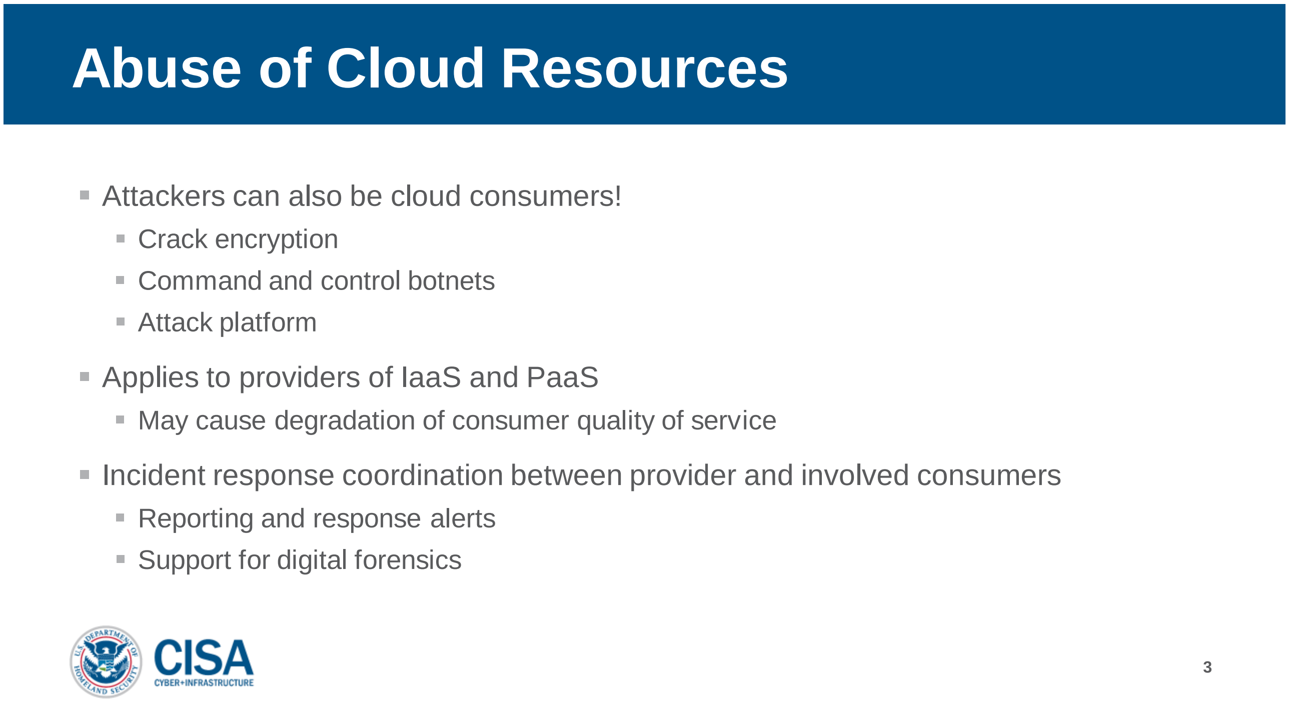
- Malicious or accidental theft, disclosure, erasure, and/or modification
- High-value data includes:
  - Financial information
  - Health and Identity information
  - Intellectual property
- Examples too numerous to name
- Mitigations: Multi-factor authentication, encryption, isolation
  - Change of cloud deployment model
- Provider is generally not responsible for consumer data
  - Service Level Agreements

**002 The first threat on everyone's mind when we talk about the cloud is data breaches and data loss. Unfortunately, examples of this are entirely too numerous to name. Data breaches occur when there is accidental or deliberate theft of data. Data disclosure, data erasure or otherwise our data modification. High-value data can include what's on the slide. It can also include celebrity photographs or anything else that could be damaging to a particular individual or group of individuals. It's not really a unique threat to the cloud environment, it's just a unique environment for an existing threat.

Because if the cloud is breached, then you haven't just breached one consumer, you've breached multiple consumers. Because if you're able to get into one part of the cloud then it's entirely possible to break into other sections of the cloud and gain additional data. Because all of that data is being stored on a single physical space. Mitigations include multi-factor authentication. So where you can, in the public cloud turn on two factor authentication. Make sure that the cloud provider is set up to text you or email you an additional code if you access that cloud provider from an unusual location. Encryption is also one mitigation, but data encryption will only go so far if the encryption keys are also part of that data breach. Isolation is also a possibility.

So you can change from maybe a public or community cloud to a private cloud. That way you can have greater control over your data, so that your data is not lost just because the cloud provider security was lacking. And in a service level agreement with the cloud provider, the provider will generally state that it is not responsible for consumer data. That may be just a legal term but it is binding because it's in those service level agreements. So it's still on the consumer to protect the data.

Abuse of Cloud Resources



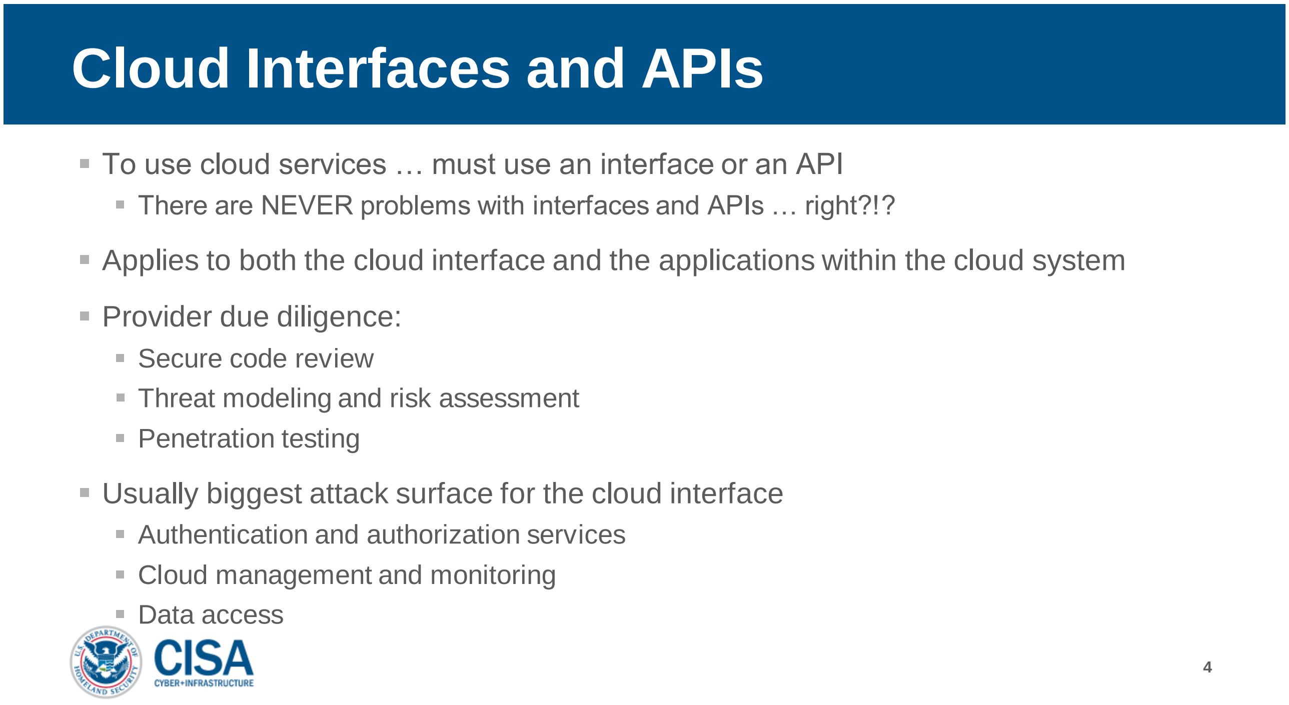
Abuse of Cloud Resources

- Attackers can also be cloud consumers!
  - Crack encryption
  - Command and control botnets
  - Attack platform
- Applies to providers of IaaS and PaaS
  - May cause degradation of consumer quality of service
- Incident response coordination between provider and involved consumers
  - Reporting and response alerts
  - Support for digital forensics

**003 The next threat a cloud we'll face is the abuse of its resources because just as regular consumers can, you know, creates their documents, share their photos, publish their blogs on a cloud resource, an attacker can rent those cloud resources for things like cracking passwords, performing those distributed denial of service attacks, and other various malicious purposes. It really applies to providers of infrastructure and platform as a service, because software as a service providers, it's really hard to abuse those resources when you only have a particular piece of software to work with. In order to perform this cracking the encryption and during the botnet command and control you really need access to additional processors and additional memory and hard drive space. And that doesn't come with a software as a service provider.

And that's where, if a cloud resources are being abused, there may be a decrease in the quality of service to other consumers. And that's where a consumer may, another consumer may alert the cloud provider to a potential abuse of resources. And then the incident response coordination has to be between the provider and any involved consumers.

Cloud Interfaces and APIs

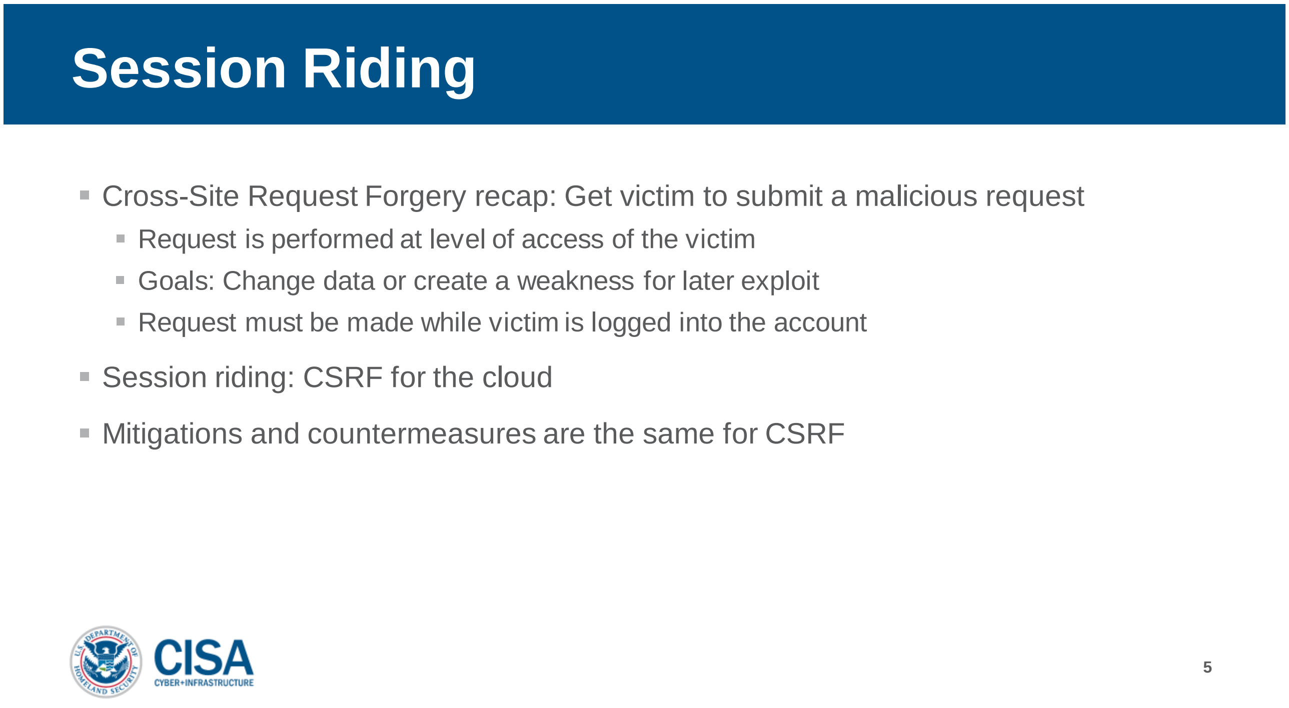


Cloud Interfaces and APIs

- To use cloud services … must use an interface or an API
  - There are NEVER problems with interfaces and APIs … right?!?
- Applies to both the cloud interface and the applications within the cloud system
- Provider due diligence:
  - Secure code review
  - Threat modeling and risk assessment
  - Penetration testing
- Usually biggest attack surface for the cloud interface
  - Authentication and authorization services
  - Cloud management and monitoring
  - Data access

**004 This next threat is again, not really unique to the cloud but it's a new and unique environment that the same old threats can be applied to. Because in order to use and manage a cloud service, you access the cloud through some kind of interface or API. And interfaces and APIs are still just software. And no piece of software is perfect. All software is going to have some kind of flaw, bug, vulnerability, what have you. So if those applications are able to be exploited, then the cloud interface can be exploited as well. And that's where this is on the cloud provider to perform some kind of due diligence on the interface and on the API that they are providing to the consumers for use. So they should, should go through secure code review. Some kind of threat modeling and risk assessment. Some kind of penetration testing. Make sure that the cloud interface and that cloud API is as secure as possible.

Session Riding

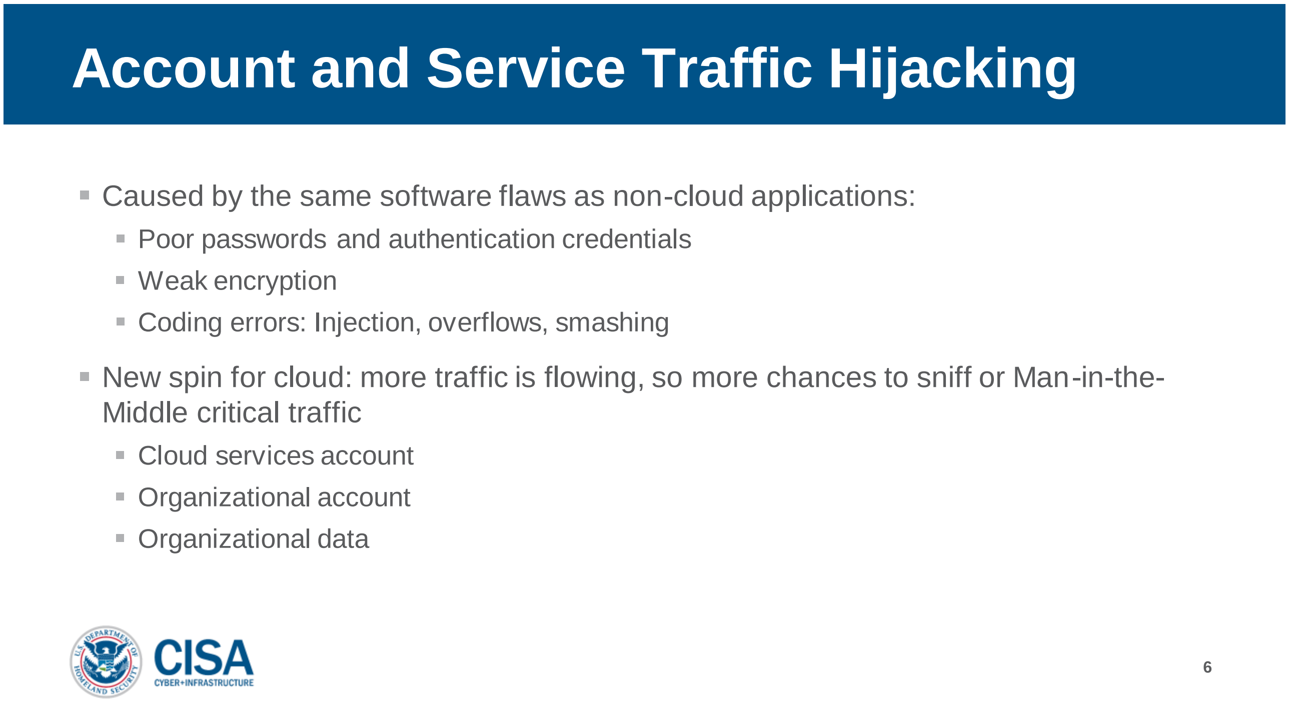


Session Riding

- Cross-Site Request Forgery recap: Get victim to submit a malicious request
  - Request is performed at level of access of the victim
  - Goals: Change data or create a weakness for later exploit
  - Request must be made while victim is logged into the account
- Session riding: CSRF for the cloud
- Mitigations and countermeasures are the same for CSRF

**005 Session writing is really cross-site request forgery under another name. Really all it is, is the cross-site request forgery for the cloud. The mitigations and the countermeasures remain the same. If you need a recap on what CSRF is, the victim establishes a communication session with a trusted site, while that trusted session is established and is active, the victim is convinced to click on to the link to open up a malicious site. That malicious site is able to sniff the credentials and sniff the session of that trusted connection and then make a request on behalf of that user. Then the trusted site doesn't know if the user has actually made that request or if being a malicious site has made that request on behalf of the user because the trusted site sees those two requests as both completely legitimate. It cannot tell the difference.

Account and Service Traffic Hijacking



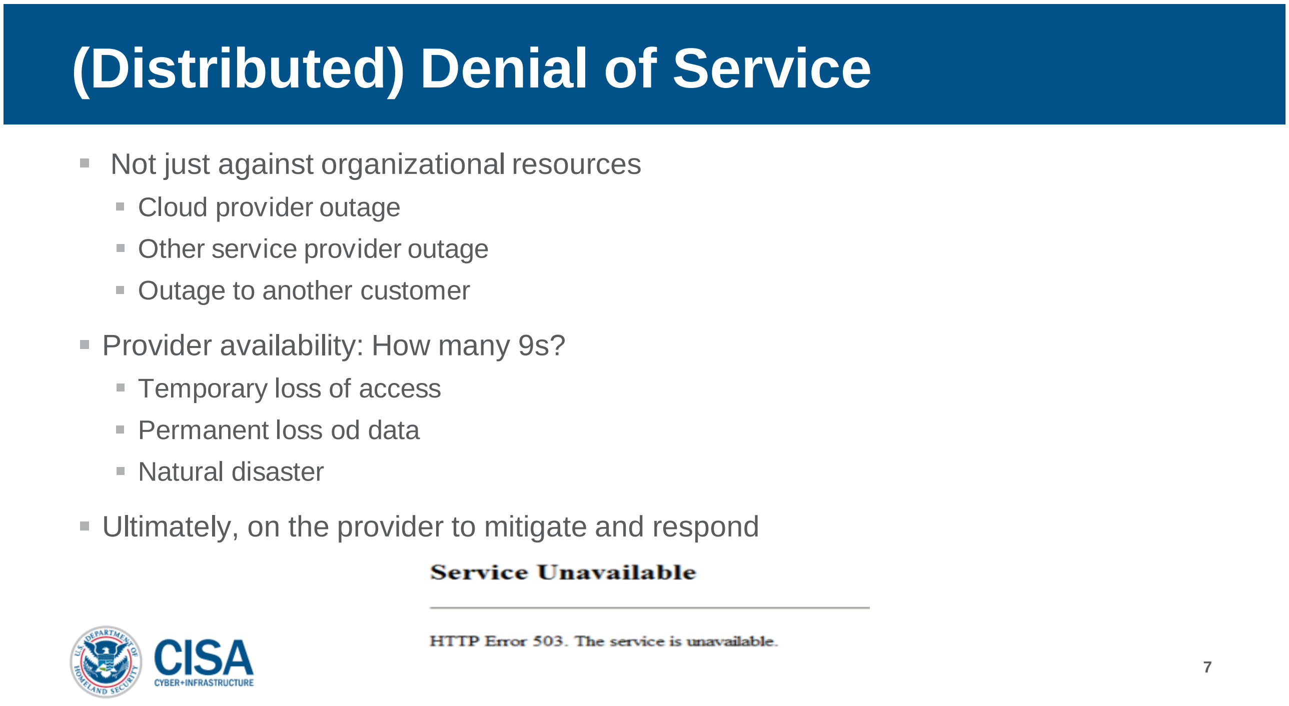
Account and Service Traffic Hijacking

- Caused by the same software flaws as non-cloud applications:
  - Poor passwords and authentication credentials
  - Weak encryption
  - Coding errors: Injection, overflows, smashing
- New spin for cloud: more traffic is flowing, so more chances to sniff or Man-in-the-Middle critical traffic
  - Cloud services account
  - Organizational account
  - Organizational data

**006 Account and service traffic hijacking. Again, same old software flaws just a new application, a new way of looking at it. So poor passwords, poor authentication credentials, improperly implemented cryptography, weak encryption practices, using say the data encryption standard instead of the triple data encryption standard, or the advanced encryption standard. Any kind of coding errors. Be it SQL injection, code injection, buffer overflows, integer overflows, stack smashing. All of those same software flaws apply to cloud applications just like they apply to non-cloud applications. Only now that we have the cloud, there are more chances to sniff critical traffic. Because we have more traffic coming over the wire we have more chances to sniff something that could be useful to an attacker.

And it's not just about the organizational account and the organizational data, there's another layer account here. Because we have an account with the cloud service provider we can potentially sniff and sort of sniff that account credential and hijack that particular account. So there's more accounts there to sniff, there's a bigger attack surface. Therefore, the threat is larger.

(Distributed) Denial of Service



(Distributed) Denial of Service

- Not just against organizational resources
  - Cloud provider outage
  - Other service provider outage
  - Outage to another customer
- Provider availability: How many 9s?
  - Temporary loss of access
  - Permanent loss od data
  - Natural disaster
- Ultimately, on the provider to mitigate and respond

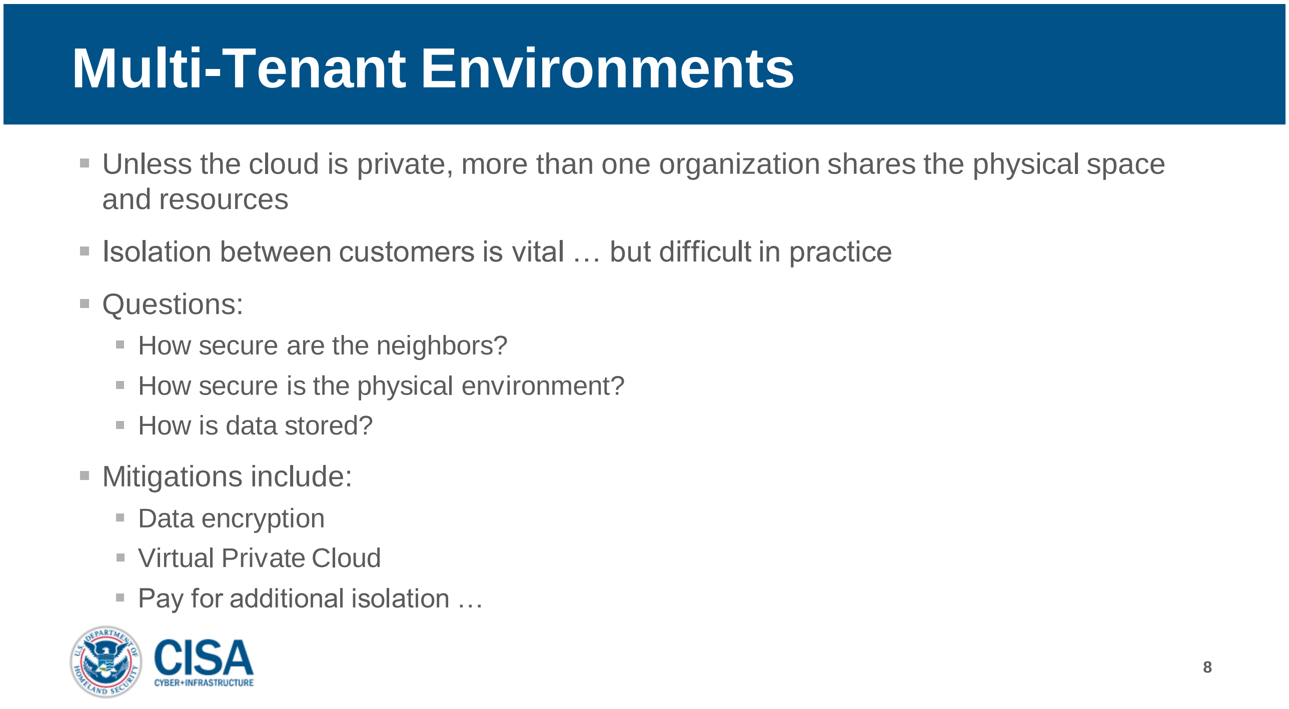
Service Unavailable

HTTP Error 503. The service is unavailable.

**007 We also have denial of service, as well as distributed denial of service. Because now it's not just applying to an organization, it's applying to that cloud provider as well, because if the cloud provider is not online then the organization is not online and none of those consumers of that particular cloud are online either. So it becomes more effective to attack the cloud provider than it does to attack any individual organization because why bother going after one organization and knocking one organization off when you can expend the same amount of resources attacking a cloud organization and affect not just 1 organization but 20 organizations. You have a bigger payoff for the same risk and the same amount of resources.

So how much does the provider have availability for? How many 9s? Is it one 9? So they have 90% uptime. Is it two 9s for 99% uptime. Is it the standard five 9s for 99.999% uptime? That's on the cloud provider to establish in that service level agreement. And it's really up to the provider to mitigate and respond to this type of attack.

Multi-Tenant Environments



Multi-Tenant Environments

- Unless the cloud is private, more than one organization shares the physical space and resources
- Isolation between customers is vital … but difficult in practice
- Questions:
  - How secure are the neighbors?
  - How secure is the physical environment?
  - How is data stored?
- Mitigations include:
  - Data encryption
  - Virtual Private Cloud
  - Pay for additional isolation …

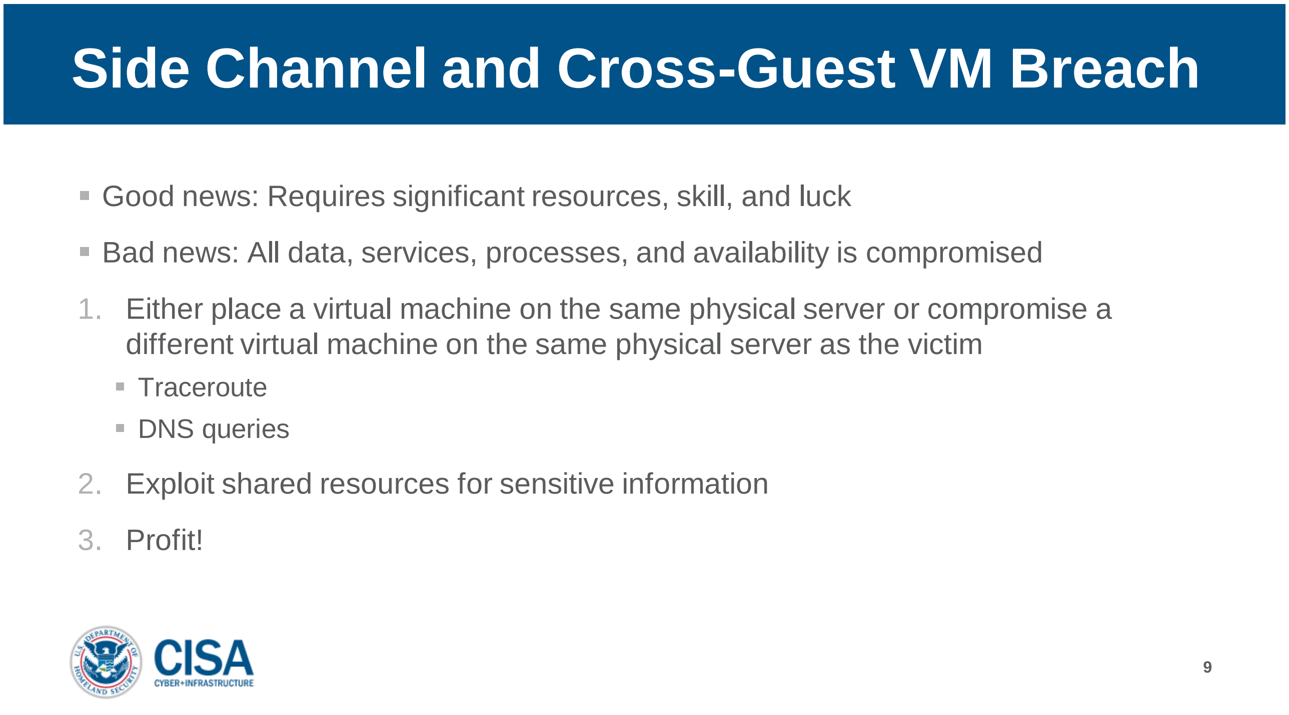
CISA
CYBER+INFRASTRUCTURE

8

**008 The two are very related. First off, we have multi-tenant environments. So what this is, is unless the cloud is private then more than one organization shares that physical space. Kind of what the cloud's for right. We're renting space so that we don't have to buy it ourselves and establish those resources ourselves. But the cloud provider is responsible for providing some level of isolation in between different customers so that each individual customer thinks that they are the only customer of that cloud. They can't see another customer's data, they can't get at it. They don't even know that other data exists. But it does.

So how secure are the neighbors? How secure is the physical environment? Because the same as regular computer threats, if you can go over and you can touch a particular computer in the physical space you own the computer. Same thing in the cloud environment, only like I was just saying, it's bigger payoff for the same risk and the same amount of resources expended. So here you could have a virtual private cloud, you could encrypt your data, you could pay for the additional isolation, but as you get further isolated you start to lose some of the benefits that the cloud provides.

Side Channel and Cross-Guest VM Breach



Side Channel and Cross-Guest VM Breach

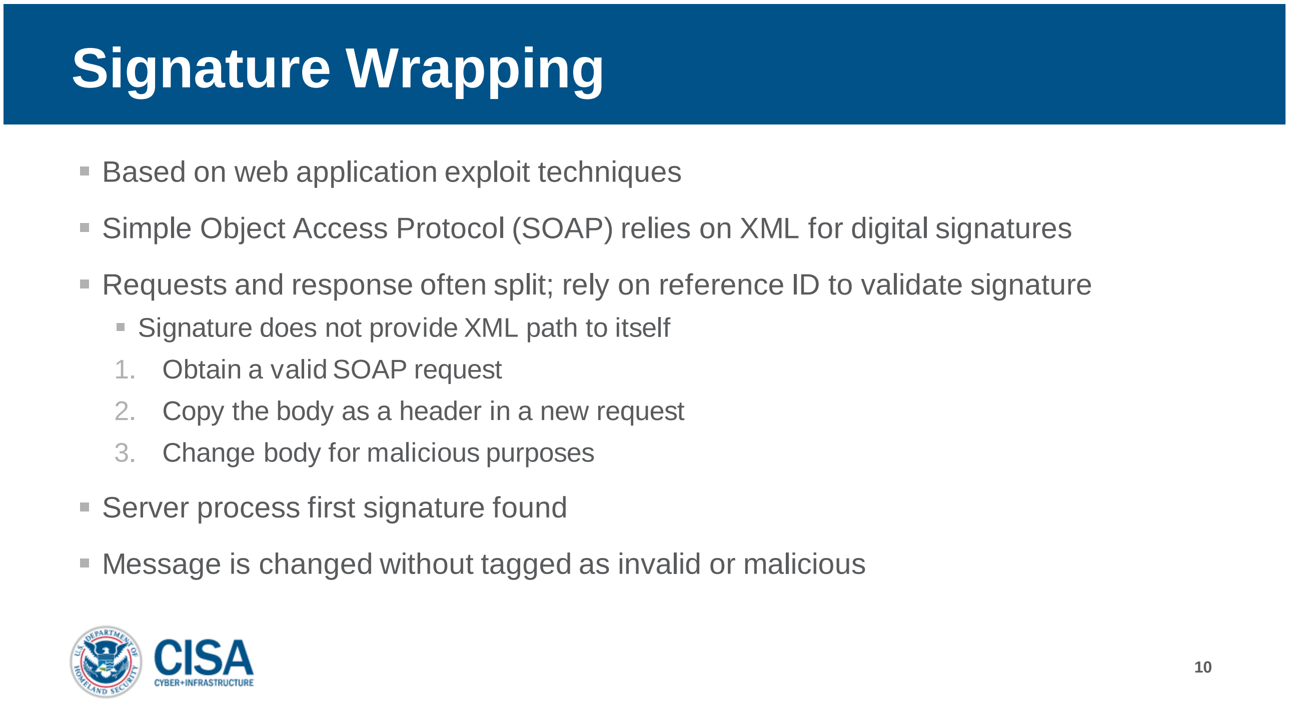
- Good news: Requires significant resources, skill, and luck
- Bad news: All data, services, processes, and availability is compromised

1. Either place a virtual machine on the same physical server or compromise a different virtual machine on the same physical server as the victim
   - Traceroute
   - DNS queries
2. Exploit shared resources for sensitive information
3. Profit!

**009 And the reason why multi-tenant environments are a big deal is because of cross guest VM breaches and side channel attacks. The good news here is that these attacks do require a significant amount of resources to pull off, as well as a significant level of skill, and just a dash of luck as well. The bad news is that if these attacks are successful, the entire physical host is compromised and every single customer is compromised. All the data is compromised. It's game over. Three basic steps here. We have to place a virtual machine on the same physical server, or compromise a virtual machine on that physical server. So the attacker has control of the virtual machine, on the same physical server that they want to breach into, their actual target. So they're in the same physical space as their target. Then all they have to do, and I say all they have to do, is exploit the shared resources in between those two tenants to be able to access sensitive information.

So if they're able to break out of their virtual machine and into somebody else's virtual machine, basically shattering the walls between two customers, then they can access sensitive information that maybe they shouldn't have access too. And then of course our third step is profiting from that information.

Signature Wrapping



Signature Wrapping

- Based on web application exploit techniques
- Simple Object Access Protocol (SOAP) relies on XML for digital signatures
- Requests and response often split; rely on reference ID to validate signature
  - Signature does not provide XML path to itself
  1. Obtain a valid SOAP request
  2. Copy the body as a header in a new request
  3. Change body for malicious purposes
- Server process first signature found
- Message is changed without tagged as invalid or malicious

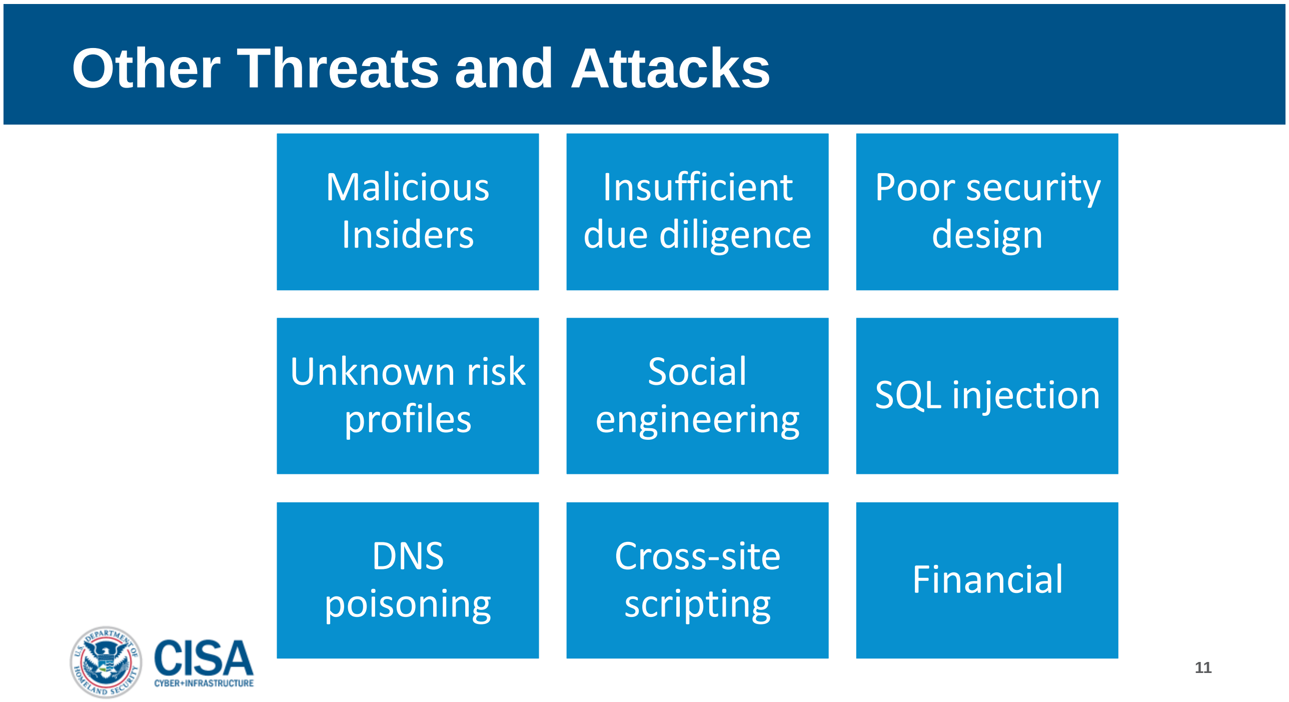
CISA CYBER+INFRASTRUCTURE

**010 Our next attack is signature wrapping. And this is really the same as web application exploitation techniques. We're going back to using SOAP that simple object access protocol that XML relies on to provide visual signatures. Only the thing is the SOAP request and response are split up. So there's only a reference ID to tie that request to that response. And that signature file? It doesn't provide the full path back to itself. It only provides a relative path back to itself. So a smart attacker can go in there and take advantage of the fact that that whole path is not specified. If you can obtain a valid request, you copy that valid request, you take the valid body, put it in the header of the new request and then change the body of your malicious request for your own purposes. So let me draw that out so it makes more sense.

So we have a completely valid request. We have the head and we have the body. And somehow the attacker has compromised this information. So in the malicious request, which I will label as invalid, we have the valid head and the valid body as part of the header of the new request. So all of this is the header. And then this section, the body will be invalid in nature. And that's where the malicious code will take place.

And the trick to this is that the server processes the first signature it finds. So it will process the valid request, valid signature that it finds, and the header of the invalid request and will take that invalid request and treat it as completely valid.

Other Threats and Attacks



Other Threats and Attacks

Malicious Insiders	Insufficient due diligence	Poor security design
Unknown risk profiles	Social engineering	SQL injection
DNS poisoning	Cross-site scripting	Financial

**011 There are other threats and other attacks. Cloud computing is not necessarily a unique platform for some of these attacks, as DNS poisoning can still happen. We can still have cross-site scripting. We can still have malicious insiders. We can still have social engineering and SQL injection. All of these same threats and these same attacks still apply to a cloud environment.

Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT D] Distribution authorized to the Department of Defense and U.S. DoD contractors only (administrative or operational use) (2016-05-01). Other requests shall be referred to DISA/RME.

DM-0004104