6.033 Spring 2018
Lecture #20

• Introduction to security
  • Threat models, policy
  • Guard model
Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN - 4/24/2018, 3:00 PM

Amazon lost control of a small number of its cloud services IP addresses for two hours on Tuesday morning when hackers exploited a known Internet-protocol weakness that let them redirect traffic to rogue destinations. By subverting Amazon's domain-resolution service, the attackers masqueraded as cryptocurrency website MyEtherWallet.com and stole about 118.68 bitcoin, or $1.3 million at the time, according to security researchers.

© Condé Nast. All rights reserved. This content is excluded from our Creative Commons license. For more information, see https://ocw.mit.edu/help/faq-fair-use.
Yahoo says half a billion accounts breached by nation-sponsored hackers

One of the biggest compromises ever exposes names, e-mail addresses, and much more.

DAN GOODIN - 9/22/2016, 4:21 PM
SNEAKY EXPLOIT ALLOWS PHISHING ATTACKS FROM SITES THAT LOOK SECURE
Phishing with Unicode Domains

Posted by Xudong Zheng on April 14, 2017

Before I explain the details of the vulnerability, you should take a look at the proof-of-concept.

Punycode makes it possible to register domains with foreign characters. It works by converting individual domain label to an alternative format using only ASCII characters. For example, the domain "xn--s7y.co" is equivalent to "短.co".

From a security perspective, Unicode domains can be problematic because many Unicode characters are difficult to distinguish from common ASCII characters. It is possible to register domains such as "xn--pple-
BrickerBot, the permanent denial-of-service botnet, is back with a vengeance

New botnet squadrons wage fiercer, more intense attacks on unsecured IoT devices.

DAN GOODIN  4/24/2017, 4:43 PM
The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought

MICHAEL B KELLEY  |  NOV. 20, 2013, 12:58 PM  |  60,330  |  11

The Stuxnet virus that ravaged Iran's Natanz nuclear facility "was far more dangerous than the cyberweapon that is now
In-flight Wi-Fi is “direct link” to hackers
Report: Planes could be targeted by a malicious hacker on the ground.

by Michael Rundle Apr 15, 2015 11:03am EDT

© Condé Nast. All rights reserved. This content is excluded from our Creative Commons license. For more information, see https://ocw.mit.edu/help/faq-fair-use.
Meet the e-voting machine so easy to hack, it will take your breath away

Virginia decertifies device that used weak passwords and wasn't updated in 10 years.

by Dan Goodin - Apr 15, 2015 2:55pm EDT

The promise—and massive challenge—of making games for the Apple Watch

How to make 15-second microgames with targets "the size of salad bar ham cubes"
what makes computer security special?
why is security difficult?
steps towards building a more secure system:

1. be clear about goals (policy)
2. be clear about assumptions (threat model)
**complete mediation**: every request for resource goes through the guard

**authentication**: is the principal who they claim to be?

**authorization**: does principal have access to perform request on resource?
what can go wrong with the guard model?
**sql injection demo**

<table>
<thead>
<tr>
<th>username</th>
<th>email</th>
<th>public?</th>
</tr>
</thead>
<tbody>
<tr>
<td>karen</td>
<td><a href="mailto:karen@fake.com">karen@fake.com</a></td>
<td>yes</td>
</tr>
<tr>
<td>peter</td>
<td><a href="mailto:peter@fake.com">peter@fake.com</a></td>
<td>yes</td>
</tr>
<tr>
<td>katrina</td>
<td>no</td>
<td></td>
</tr>
</tbody>
</table>

```sql
SELECT username, email FROM users WHERE username='<username>' AND public='yes'

Let <username> = katrina' OR username='
sql injection demo

<table>
<thead>
<tr>
<th>username</th>
<th>email</th>
<th>public?</th>
</tr>
</thead>
<tbody>
<tr>
<td>karen</td>
<td><a href="mailto:karen@fake.com">karen@fake.com</a></td>
<td>yes</td>
</tr>
<tr>
<td>peter</td>
<td><a href="mailto:peter@fake.com">peter@fake.com</a></td>
<td>yes</td>
</tr>
<tr>
<td>katrina</td>
<td>no</td>
<td></td>
</tr>
</tbody>
</table>

SELECT username, email FROM users WHERE username='\textit{katrina}' OR username='\textit{}' AND public='\textit{yes}'
cd /mit/bob/project

cat ideas.txt

Hello world.

...

mail alice@mit.edu < ideas.txt
what can go wrong with the guard model?
• **Adversarial attacks** are different from “normal” failures. They’re targeted, rarely random, and rarely independent. Just one successful attack can bring down a system.

• Securing a system starts by specifying our goals (**policy**) and assumptions (**threat model**).

• The **guard model** provides **complete mediation**. Even though things can still go wrong, systems that use this model avoid common pitfalls.