6.033 Spring 2017
Lecture #20

- Introduction to security
- Threat models, policy
- Guard model
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](https://www.apple.com).

**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-
Risk Assessment —

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

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
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
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)*
guard model of security

provides **complete mediation**. Systems that use this model avoid common pitfalls.
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>melva</td>
<td><a href="mailto:melva@mit.edu">melva@mit.edu</a></td>
<td>yes</td>
</tr>
<tr>
<td>peter</td>
<td><a href="mailto:psz@mit.edu">psz@mit.edu</a></td>
<td>yes</td>
</tr>
<tr>
<td>katrina</td>
<td><a href="mailto:lacurts@mit.edu">lacurts@mit.edu</a></td>
<td>no</td>
</tr>
</tbody>
</table>

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>melva</td>
<td><a href="mailto:melva@mit.edu">melva@mit.edu</a></td>
<td>yes</td>
</tr>
<tr>
<td>peter</td>
<td><a href="mailto:psz@mit.edu">psz@mit.edu</a></td>
<td>yes</td>
</tr>
<tr>
<td>katrina</td>
<td><a href="mailto:lacurts@mit.edu">lacurts@mit.edu</a></td>
<td>no</td>
</tr>
</tbody>
</table>

```sql
SELECT username, email FROM users WHERE username='katrina' OR username=''
    AND public='yes'
```
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.