6.033 Spring 2016
Lecture #20

- Introduction to security
- Threat models, policy
- Guard model
How hackers eavesdropped on a US Congressman using only his phone number
SS7 routing protocol also exposes locations, contacts, and other sensitive data.

by Dan Goodin - Apr 18, 2016 7:19pm EDT
Los Angeles Hospital Pays Hackers $17,000 After Attack

By STACY COWLEY and LIAM STACK  FEB. 18, 2016
Bank Botnets Continue to Thrive One Year After Gameover Zeus Takedown

Features on new botnets suggest attackers have learned from the lessons of takedown.

RSA CONFERENCE -- San Francisco -- Despite the takedowns of the Gameover Zeus and Shylock botnets last year, banking botnet activity continues to persist unabated.

If anything, they have become even more sophisticated and evasive suggesting that those behind these botnets have learned and adapted from the Zeus and Shylock takedowns, a report from Dell SecureWorks Counter Threat Unit said Wednesday.
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

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*)
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>matei</td>
<td><a href="mailto:matei@mit.edu">matei@mit.edu</a></td>
<td>yes</td>
</tr>
<tr>
<td>mike</td>
<td><a href="mailto:mcarbin@mit.edu">mcarbin@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>matei</td>
<td><a href="mailto:matei@mit.edu">matei@mit.edu</a></td>
<td>yes</td>
</tr>
<tr>
<td>mike</td>
<td><a href="mailto:mcarbin@mit.edu">mcarbin@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'
```
> 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.