6.033 Spring 2015

Lecture #21

- **Introduction to security**
  - **Threat models, policy**
  - **Guard model**

Katrina LaCurts | lacurts@mit | 6.033 2015

FCC: AT&T Workers Stole ...

fortune.com/2015/04/08/att-workers-data-breach/

TIME INC. NETWORK : FORTUNE MONEY TIME SPORTS ILLUSTRATED GOLF TRAVEL + LEISURE MORE

MENU FORTUNE SUBSCRIBE

APRIL 25, 2015
Solar-powered drones could spy on Earth (and explore other planets)

NEWS POPULAR VIDEOS RANKINGS

AT&T workers stole almost 280,000 customers' personal data: FCC APRIL 8, 2015

Apple analysts scramble to raise their iPhone estimates 12:57 PM EDT

How much would you sacrifice to start your own business? 11:00 AM EDT

Solar power will soon make it possible to fly planes continuously—but is that a good thing? 10:30 AM EDT

Billionaires versus big oil 9:00 AM EDT

Yes, there are craft beers made with testicles, Peeps, and, um, poop 8:00 AM EDT

AT&T workers stole almost 280,000 customers' personal data: FCC

by Benjamin Snyder @WriterSnyder APRIL 8, 2015, 3:26 PM EDT

Let the phishing begin: Sc...

arstechnica.com/security/2015/02/09/let-the-phishing-begin-scammers-now-targeting-anthem-hack-victims/

Register Log in

ars technica

MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS ARS CONSORTIUM

RISK ASSESSMENT / SECURITY & HACKTIVISM

Let the phishing begin: Scammers now targeting Anthem hack victims

E-mails promising free credit monitoring pour salt in wounds of Anthem victims.

by **Dan Goodin** - Feb 9, 2015 10:44am EST

Share Tweet 34

Less than a week after health insurer Anthem warned that a breach of its network exposed the personal information of as many as 80 million people, scammers are sending phishing e-mails that target those unlucky individuals.

The fraudulent e-mails claim they are official Anthem communications being sent to current and former customers. The messages promise free credit monitoring services for people who click on a link that asks for personal data.

"This outreach is from scam artists who are trying to trick consumers into sharing personal data," Anthem officials wrote in an advisory. "There is no indication that the scam e-mail campaigns are being conducted by those that committed the cyber attack, or that the information accessed in the attack is being used by the scammers."

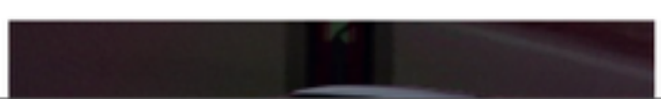
LATEST FEATURE STORY

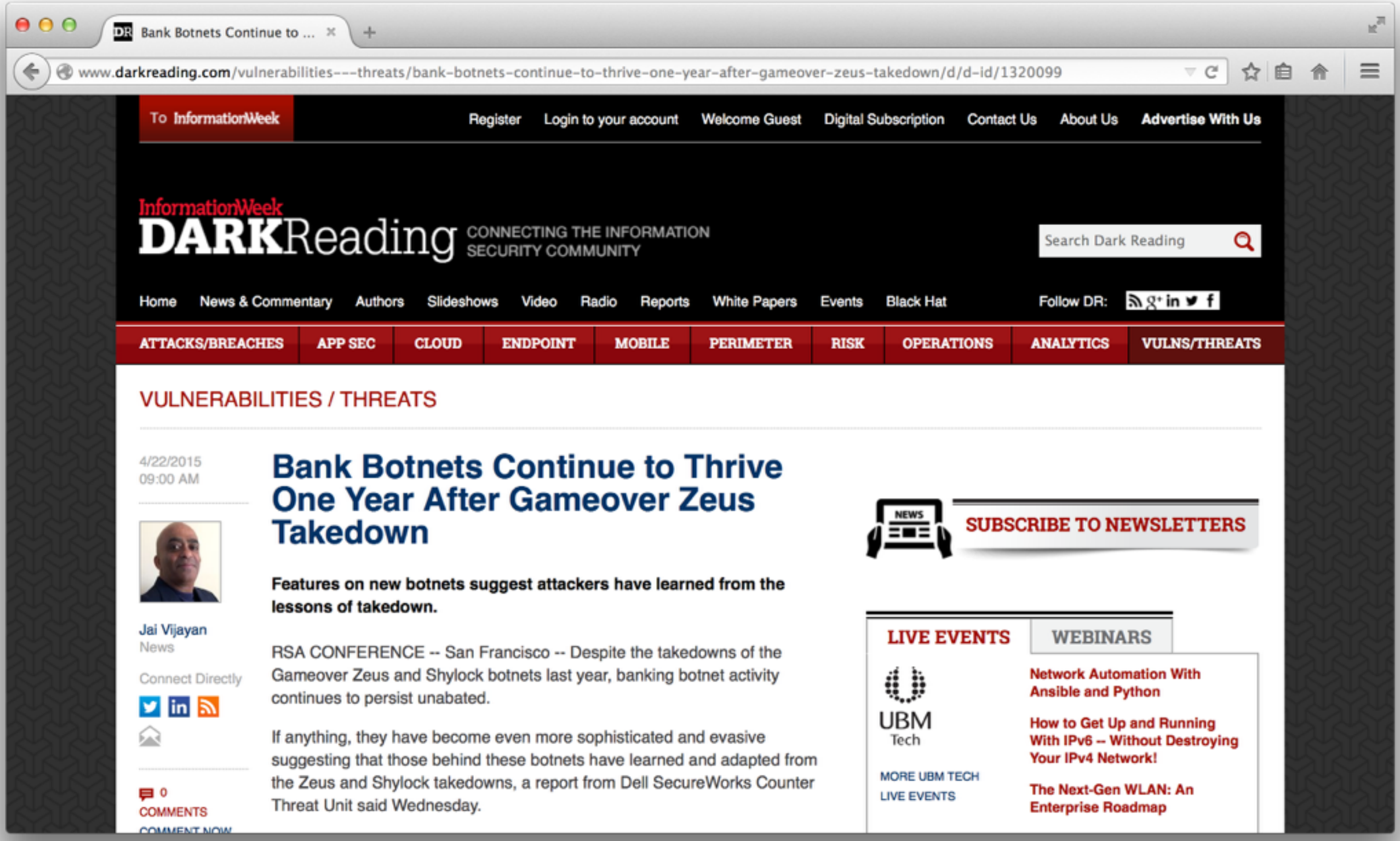
FEATURE STORY (2 PAGES)

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"

WATCH ARS VIDEO




Bank Botnets Continue to ...
www.darkreading.com/vulnerabilities---threats/bank-botnets-continue-to-thrive-one-year-after-gameover-zeus-takedown/d/d-id/1320099
To InformationWeek
Register
Login to your account
Welcome Guest
Digital Subscription
Contact Us
About Us
Advertise With Us
InformationWeek
DARKReading
CONNECTING THE INFORMATION SECURITY COMMUNITY
Search Dark Reading
Home
News & Commentary
Authors
Slideshows
Video
Radio
Reports
White Papers
Events
Black Hat
Follow DR:
ATTACKS/BREACHES
APP SEC
CLOUD
ENDPOINT
MOBILE
PERIMETER
RISK
OPERATIONS
ANALYTICS
VULNS/THREATS
VULNERABILITIES / THREATS
4/22/2015
09:00 AM
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.
Jai Vijayan
News
Connect Directly
0
COMMENTS
COMMENT NOW
NEWS
SUBSCRIBE TO NEWSLETTERS
LIVE EVENTS
WEBINARS
UBM Tech
MORE UBM TECH LIVE EVENTS
Network Automation With Ansible and Python
How to Get Up and Running With IPv6 -- Without Destroying Your IPv4 Network!
The Next-Gen WLAN: An Enterprise Roadmap

Stuxnet Was Far More Dan...

www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

BUSINESS INSIDER

BI INTELLIGENCE EVENTS LOGIN REGISTER US EDITION

Tech Finance Politics Strategy Life Sports Video All Search

MILITARY & DEFENSE

More: Stuxnet Iran Israel Cyberwarfare

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

FACEBOOK LINKEDIN TWITTER

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 li...

arstechnica.com/security/2015/04/15/in-flight-wi-fi-is-direct-link-to-hackers/

Register Log in

ars technica

MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS ARS CONSORTIUM

RISK ASSESSMENT / SECURITY & HACKTIVISM

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

Share Tweet 88

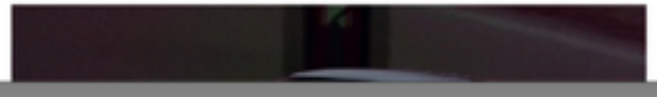
LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

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"

WATCH ARS VIDEO



Meet the e-voting machin...

arstechnica.com/tech-policy/2015/04/15/meet-the-e-voting-machine-so-easy-to-hack-it-will-take-your-breath-away/

Register Log in

ars technica

MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS ARS CONSORTIUM

LAW & DISORDER / CIVILIZATION & DISCONTENTS

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

Share Tweet 156

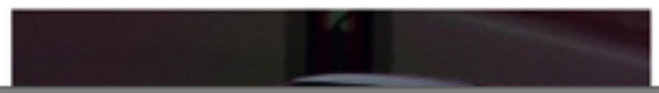
LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

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"

WATCH ARS VIDEO



what makes computer security special?

Katrina LaCurts | lacurts@mit | 6.033 2015

why is security difficult?

Katrina LaCurts | lacurts@mit | 6.033 2015

steps towards building a more secure system:

1. be clear about goals (policy)
2. be clear about assumptions (threat model)

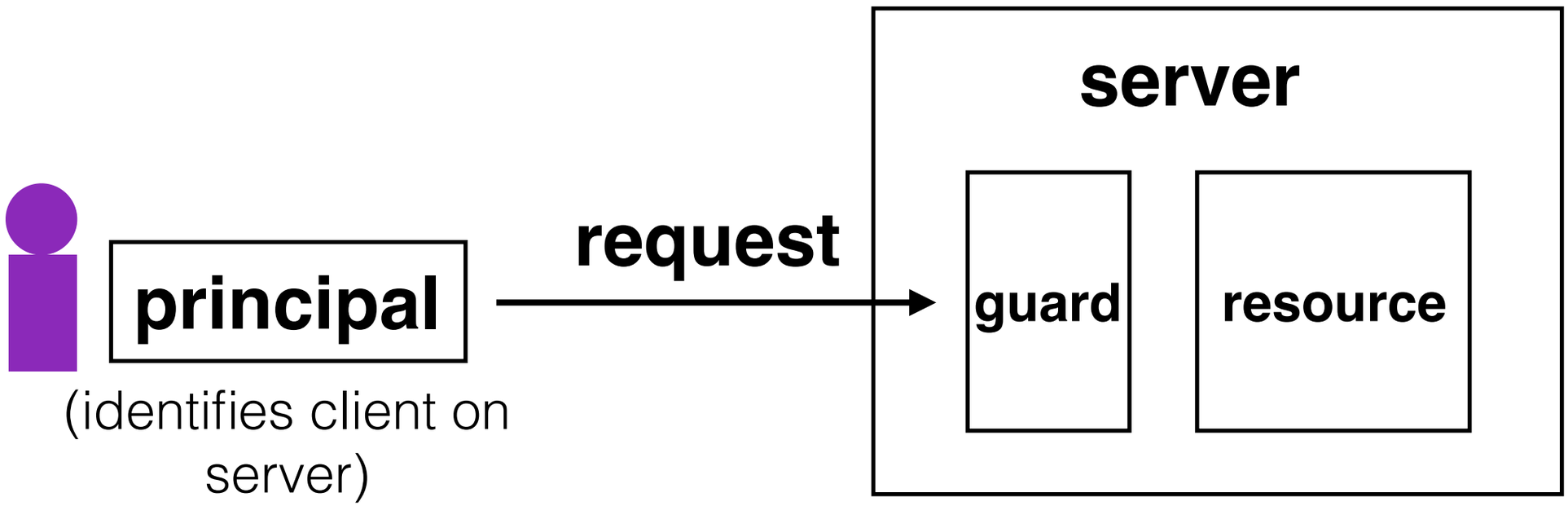
guard model of security

provides **complete mediation**.

systems that use this model avoid common pitfalls

Katrina LaCurts | lacurts@mit | 6.033 2015

complete mediation: every request for resource goes through the guard



guard typically provides:

authorization: does principal have access to perform request on resource?

authentication: is the principal who they claim to be?

what can go wrong with the guard model?

Katrina LaCurts | lacurts@mit | 6.033 2015

sql injection demo

username	email	public?
hari	hari@csail.mit.edu	yes
sam	madden@csail.mit.edu	yes
katrina	katrina@csail.mit.edu	no

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

inputting the username `katrina' OR username='` changes the query to:

```
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
```

- **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.