6.033 Spring 2019

Lecture #20

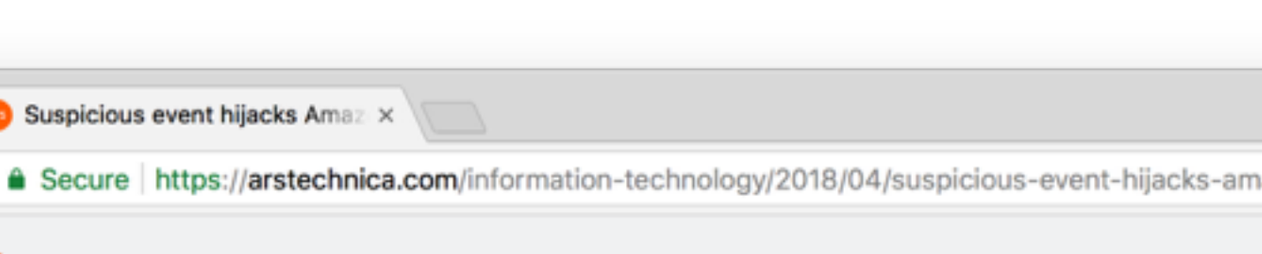
- **Introduction to security**
  - **Threat models, policy**
  - **Guard model**

BORDER GATEWAY PROTOCOL ATTACK —

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

108

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 to redirect traffic to rogue destinations. By subverting Amazon's domain-resolution service, the attackers masqueraded as cryptocurrency website MyEtherWallet.com and stole about

RISK ASSESSMENT —

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.

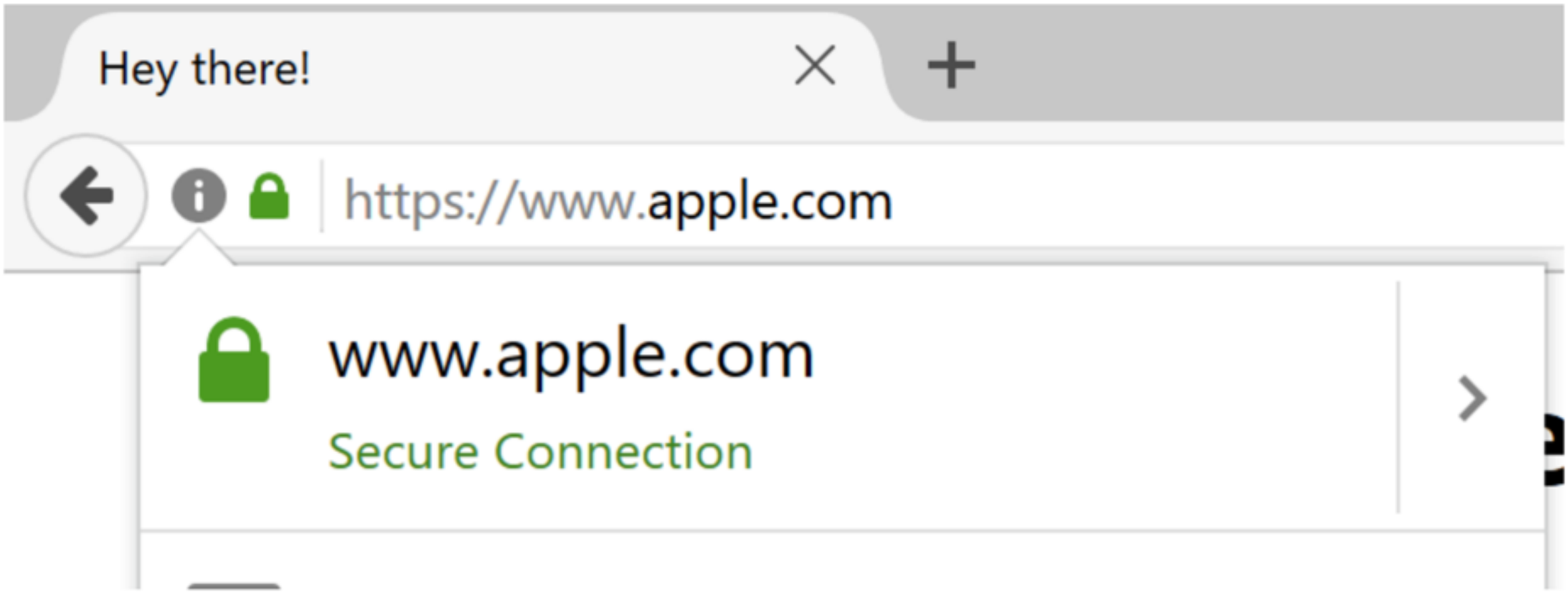
DAN GOODIN - 9/22/2016, 4:21 PM

LILY HAY NEWMAN SECURITY 04.18.17 7:00 AM

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-

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

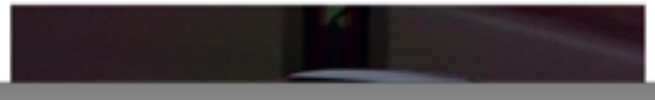
LATEST FEATURE STORY

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 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

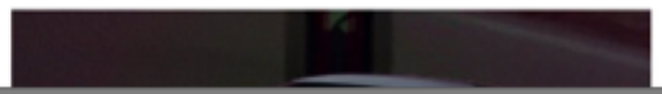
LATEST FEATURE STORY

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



Chips may be inherently vulner

https://www.technologyreview.com/s/612989/chips-may-be-inherently-vulnerable-to-spectre-and-meltdown-attacks/

Chips may be inherently vulnerable to Spectre and Meltdown attacks

SONGSAK WILAIRIT / EYEEM

Computing

Chips may be inherently vulnerable to Spectre and Meltdown attacks

Most malware exploits coding errors and poor design. But Google security researchers say a fundamental flaw in the nature of computing could make some threats impossible to defeat.

by **Emerging Technology from the arXiv** Feb 05

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

The Stuxnet virus that ravaged Iran's Natanz nuclear facility "was far more dangerous than the cyberweapon that is now

The 5 Worst Examples of IoT H

https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

iot for all

TECH IOT EXPLAINED PODCAST N

Home › Insights

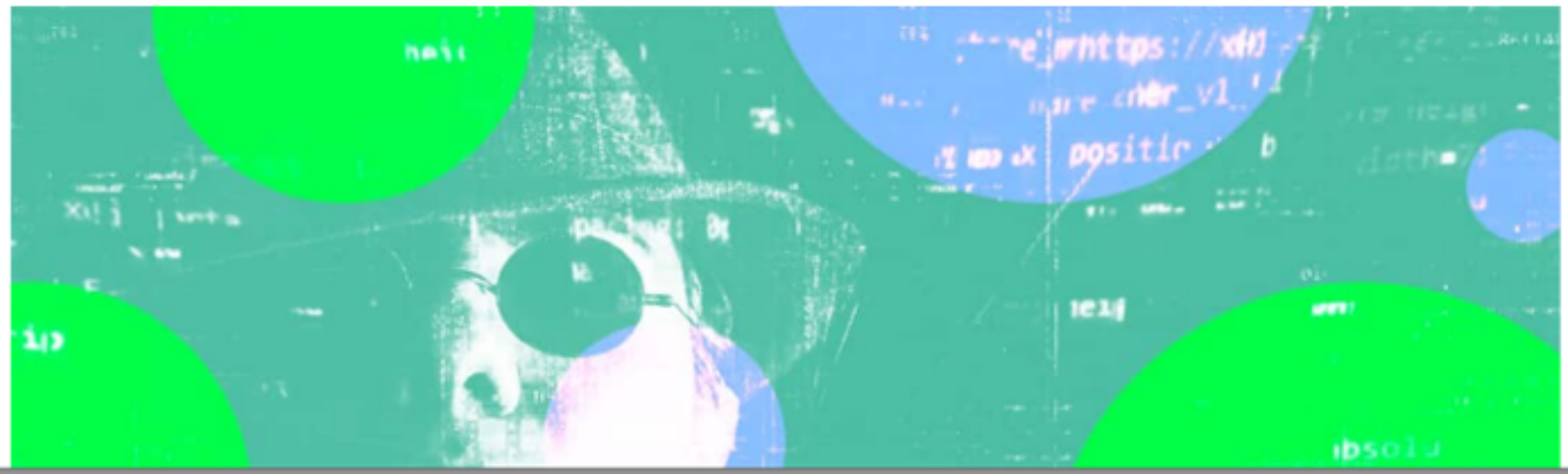
Insights Internet of Things Security

The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History

IoT hacking can be extremely effective, producing DDoS attacks that can cripple our infrastructure, systems, and way of life.

By **Guest Writer** - May 10, 2017

115958



1. The Mirai Botnet (aka Dyn Attack)

Back in October of 2016, the largest DDoS attack ever was launched on service provider Dyn using an IoT botnet. This lead to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN.

2. The Hackable Cardiac Devices from St. Jude

Early last year, CNN wrote, "The FDA confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities that could allow a hacker to access a device. Once in, they could deplete the battery or administer incorrect pacing or shocks, the FDA said.

3. The Owlet WiFi Baby Heart Monitor Vulnerabilities

Right behind the St. Jude cardiac devices is the Owlet WiFi baby heart monitor.

According to Cesare Garlati, Chief Security Strategist at the prpl Foundation:

"This latest case is another example of how devices with the best of intentions, such as alerting parents when their babies experience heart troubles, can turn dangerous if taken advantage of by a sinister party.

4. The TRENDnet Webcam Hack

And, continuing with the baby theme, TechNewsWorld reports, "TRENDnet marketed its SecurView cameras for various uses ranging from home security to baby monitoring and claimed they were secure, the FTC said. However, they had faulty software that let anyone who obtained a camera's IP address look through it — and sometimes listen as well.

5. The Jeep Hack

The IBM security intelligence website reported the Jeep hack a few years ago, saying, "It was just one, but it was enough. In July [2015], a team of researchers was able to take total control of a Jeep SUV using the vehicle's CAN bus.

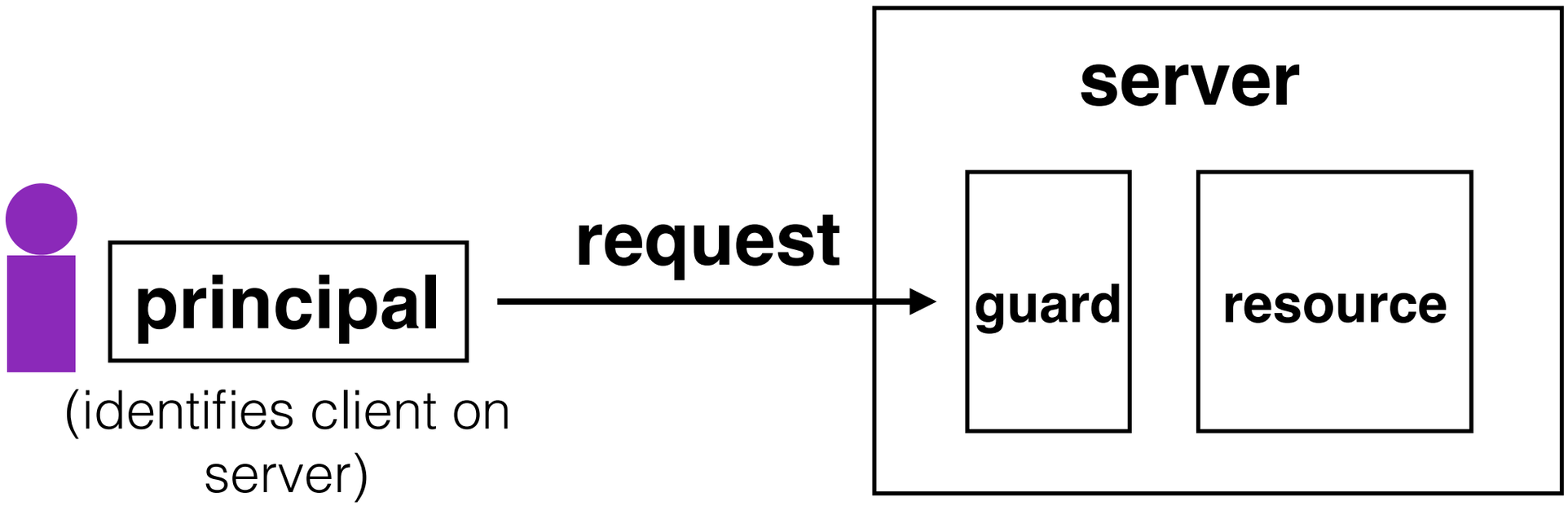
what makes computer security special?

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

username	email	public?
karen	sollins@mit.edu	yes
olivia	nibr@mit.edu	yes
katrina	lacurts@mit.edu	no

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

Let `<username>` = `katrina' OR username='`

sql injection demo

username	email	public?
karen	sollins@mit.edu	yes
olivia	nibr@mit.edu	yes
katrina	lacurts@mit.edu	no

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

what can go wrong with the guard model?

```
> cd /mit/katie/project
> cat ideas.txt
Hello world.
...
> mail kifle@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.