6.033 Spring 2018
Lecture #20

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

1

Suspicious event hijacks Ama... ×   Katrina

← → C   🔒 Secure | https://arstechnica.com/information-technology/2018/04/suspicious-event-hijacks-amazon-traffic-for-2-hours-steals-cryptocurren... ☆ 🔲 🔲 🅡 ⋮

ars TECHNICA

BIZ & IT   TECH   SCIENCE   POLICY   CARS   GAMING & CULTURE   FORUMS   **SUBSCRIPTIONS**   🔍 ☰ SIGN IN ▾

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.com®

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
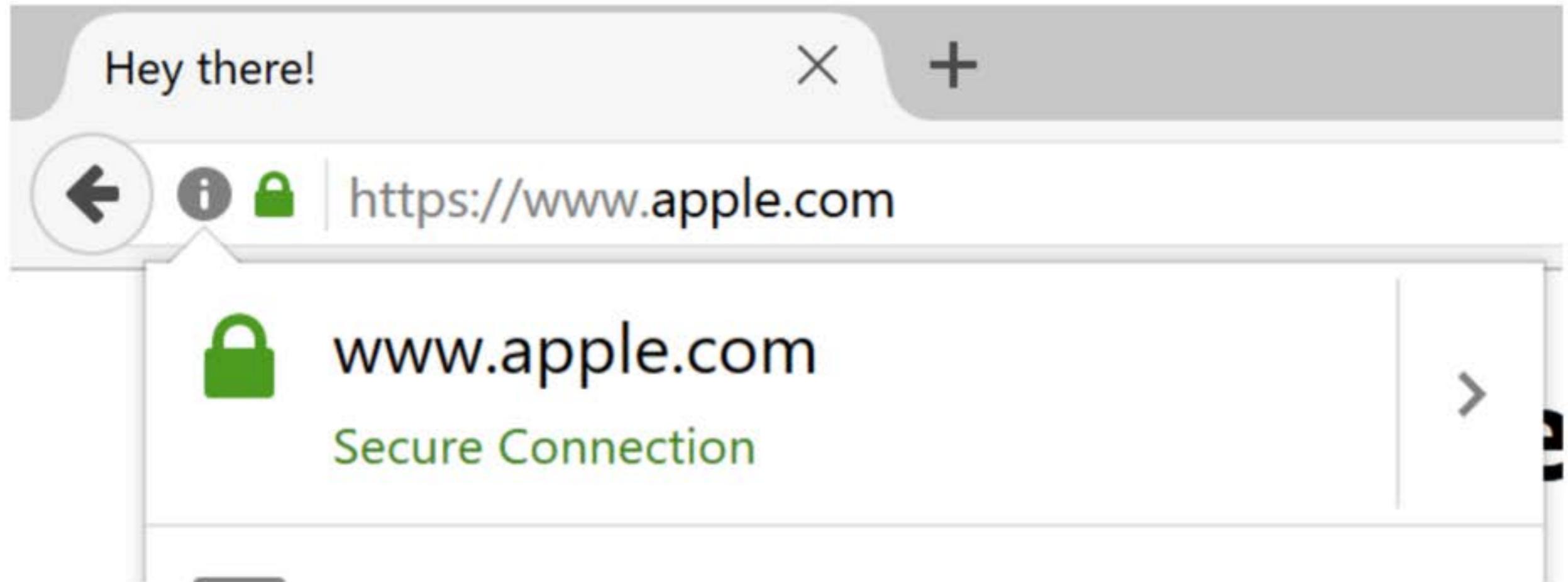
LILY HAY NEWMAN   SECURITY   04.18.17   7:00 AM

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-

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.
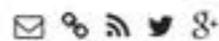
DAN GOODIN - 4/24/2017, 4:43 PM

© Insider Inc. All rights reserved. This content is excluded from our Creative Commons license. For more information, see https://ocw.mit.edu/help/faq-fair-use.
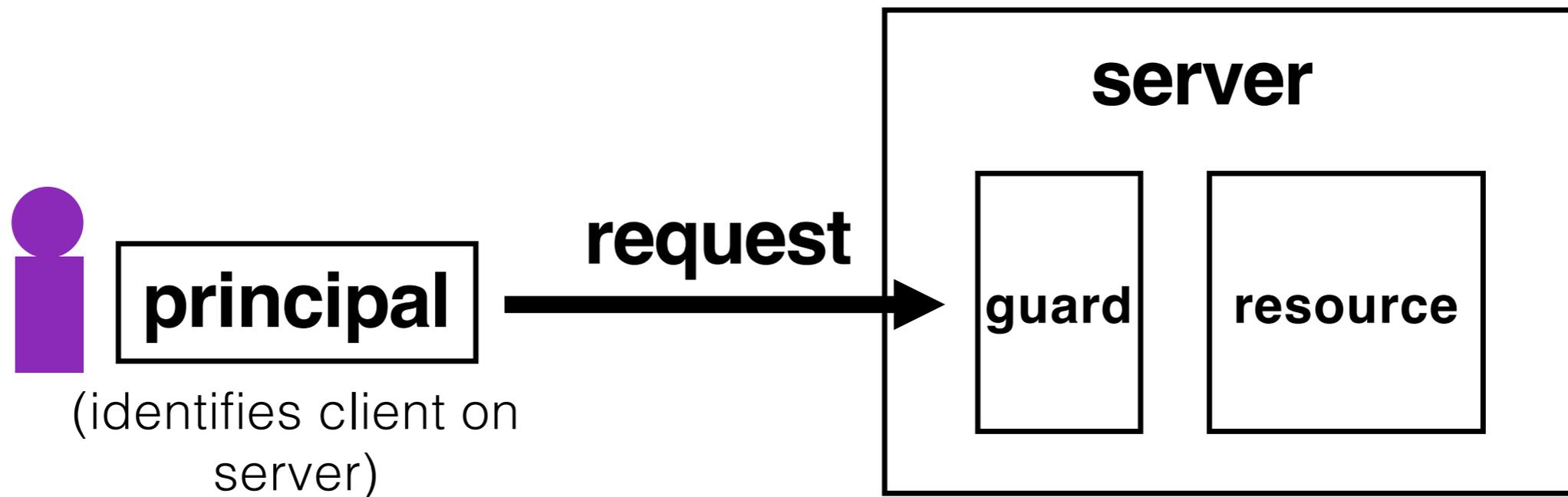
what makes computer security special?

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       | karen@fake.com      | yes
peter       | peter@fake.com      | yes
katrina     | no
```

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

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

sql injection demo

username	email	public?
karen	karen@fake.com	yes
peter	peter@fake.com	yes
katrina	**no**	

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.

6.033 Computer System Engineering
Spring 2018