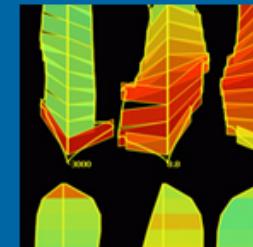
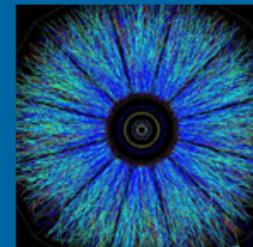
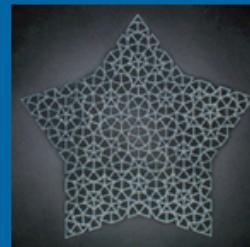
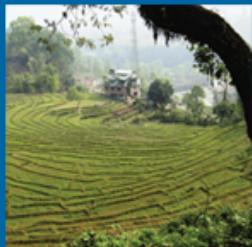




Swansea University
Prifysgol Abertawe

CS-130 Professional Issues

Threat Vectors – The Application of MalWare



Lecture Learning Goals

What is a DDOS attack and what does it look like?

What is Advanced Fee Fraud and how can you avoid it?

What is Phishing and how is it normally conducted?

What is the weakest link in any secure system?

(D)DOS Attacks to Deny Use

Destroy utility of a machine or network or resource

- Usually performed by means of a flood attack
- Can come from a single source but typically they are(d)istributed

Difficult to distinguish “Slashdoting”, “Farking”, “Drudging” or the “Reddit Hug” from DDoS

Vulnerability of home machines on connections produced armies of “zombies”

Technical, legal, and ethical responses are all difficult

Examples of (D)DOS software include LOIC and HOIC – used in famous (D)DOS attacks on, for example, Scientology websites



Got a tip? [Let us know.](#)

Follow Us [f](#) [i](#) [t](#) [y](#) [f](#) [in](#) [g+](#) [r](#)

News ▾ Video ▾ Events ▾ Crunchbase

[Message Us](#)

[Search](#)



DISRUPT BERLIN Time is running out on Early Bird savings for Disrupt Berlin [Save 30% off tickets today ▶](#)

Europe

ddos

cyber security

Brexit

Europe

Popular Posts



Tesla has fired hundreds of employees after performance reviews



eBay is having a pretty bad day



Two Google alums just raised \$60M to rethink documents

Brexit voter registration website crash could have been a DDoS, says report

Posted Apr 12, 2017 by [Natasha Lomas \(@riptari\)](#)



[Next Story ▶](#)



Crunchbase

European Union

FOUNDED
2002

OVERVIEW
The European Union occasionally makes investments. For more about them, see [their Wikipedia page] (http://en.wikipedia.org/wiki/European_Union).

LOCATION
London, England

CATEGORIES
Education, Universities, Information Services

WEBSITE
<http://europa.eu>

[Full profile for European Union](#)

Technical, legal, and ethical responses to a (D)DOS attack are all difficult... Why do you think that might be?

Advance-Fee Fraud to Steal Money

At the core of the attack is getting you to pay for something without a cast-iron guarantee in place of a return

- Intelligent, educated people can still fall for it because getting something for nothing is a powerful lure
- Comprises a significant proportion of spam and like all good “confidence tricks”, relies on greed and illegality
 - Non-refundable shipping, charge backs when selling an item online, the infamous Nigerian Prince scam

Scam-baiting

- The act of going out and baiting scammers into giving you some money
- IT'S DEFINITELY ILLEGAL!

How I Scammed The Prince Of Nigeria

⌚ 20/10/2017 12:20



Like 24



Julian Vigo

Scholar, filmmaker, artist, permaculturalist, dj, yogi, and human rights consultant



TUAN_AZIZI VIA GETTY IMAGES

In recent years I have grown accustomed to the emails legitimately soliciting new business such as appeared in my inbox this morning. Included under the spectrum of cold calling”, I received a request for car insurance, people offering to redo my website, and community updates. Not only do [surveys](#) suggest that a [majority of people](#) want to receive promotional email, but the reality is that I have on occasion

Phishing and Pharming for Personal Information or Bank Details

Phishing originally was an email pointing AOL users to a fake AOL login screen to capture login details

- Moved to other online services, particularly online banking
- Comprises a significant proportion of modern spam

Pharming uses cracked DNS servers (more on this later)

- Attacks local DNS configurations
- DNS is the Internet's equivalent of a phone book linking a URL to an IP
- But stored on local networks for commonly visited sites

What is the most powerful technique available to most hackers?



What do all of these films have in common:

“The Thomas Crown Affair”

“The Fifth Estate”

“Catch me if you can”

“Feris Bueller’s day off”

The Weakest Link: Social Engineering

Based on one simple idea: “*People want to help people*”

- The easiest way to get a users password is to ask them for it nicely
- Socially awkward interactions, phrases like “*It would just make my life much easier....*”, building personal relationships with targets
- Kevin Mitnick famously claimed that “*I never cracked a password in my life*”
- The Waterloo Study involved people swapping chocolate bars for passwords!

Social Engineering Augments Classic Attacks

Spear Phishing with Adobe/Word documents – the latest evolution of phishing and pharming

- Involves sending customised emails to a single person so they will open them with a customised Trojan
- Exploits the fact that spam filters and anti-virus needs to know about an email/Trojan to catch it

Baiting – getting malicious software onto someone's machine physically by leaving a USB lying around

- Who doesn't want a free USB stick?

MR. ROBOT

Who are Black Hats in the Real World?

Individuals or “script-kiddies” trying out hacking for fun using pre-written software

Online hacking collectives or hacktivists

- Anonymous, LulzSec, etc

Organized crime

- Links to black market distribution
- Links to online communications for offline crime

Government agencies

- Industrial espionage, influencing the course of foreign elections?

How serious does this get?

ANDY GREENBERG SECURITY 02.02.15 9:31 PM

SHARE



SHARE
86



TWEET



PIN



COMMENT
151



EMAIL

READ THE TRANSCRIPT OF SILK ROAD'S BOSS ORDERING 5 ASSASSINATIONS



GET WIRED

Don't Let The Future Leave You Behind. Get 6 Issues For Just \$5.

SUBSCRIBE NOW

MOST POPULAR



FRONTIERS
Barack Obama Talks AI, Robo-Cars, and the Future of the World

10.12.16



SECURITY
Want to Know Julian Assange's Endgame? He Told You a Decade Ago

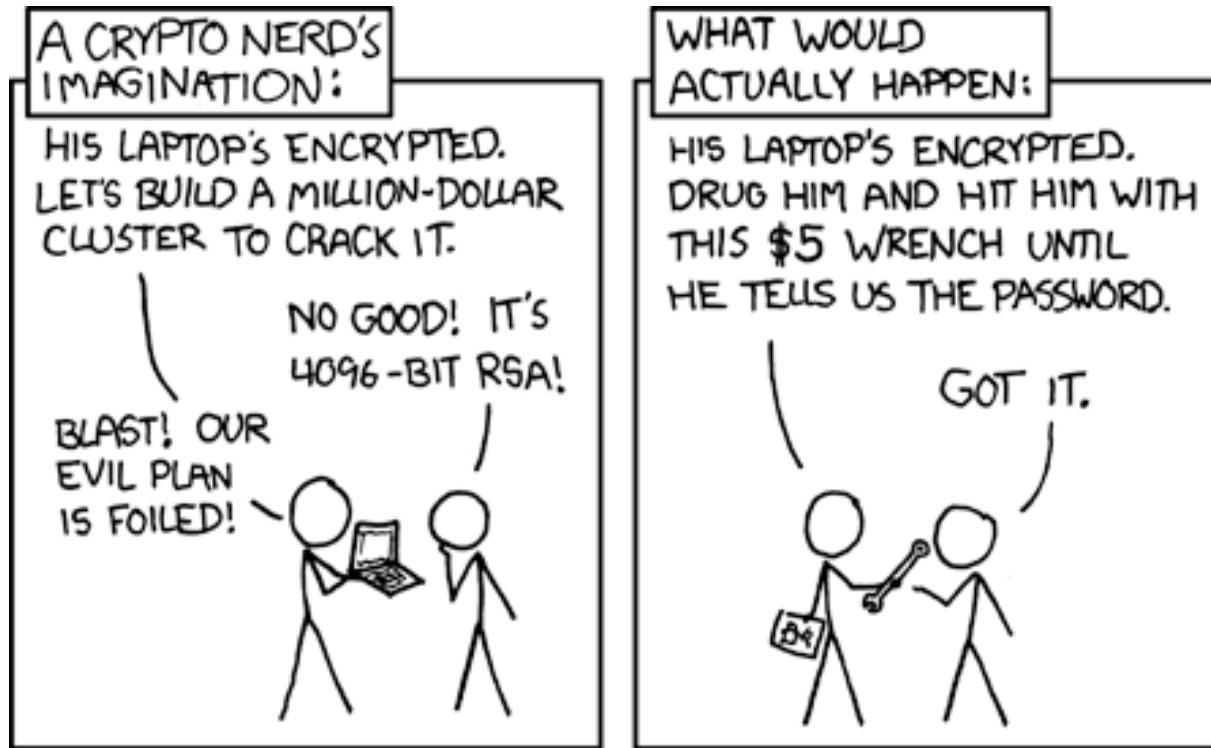
10.14.16



NATIONAL AFFAIRS
Barack Obama: Now Is the Greatest Time to Be Alive

10.12.16

A final thought....



Lecture Learning Goals

What is a DDOS attack and what does it look like?

What is Advanced Fee Fraud and how can you avoid it?

What is Phishing and how is it normally conducted?

What is the weakest link in any secure system?

Lecture Learning Goals

What is a DDOS attack and what does it look like?

Multiple computers pool resources to attack your online services and overwhelm them

What is Advanced Fee Fraud and how can you avoid it?

Giving away something for nothing, avoid it by checking the legitimacy of anyone before you transfer them money

What is Phishing and how is it normally conducted?

Email large groups of people to find a weak link

What is the weakest link in any secure system?

Authorised users (all of us) who are vulnerable to social engineering