Echavarria v. Facebook, Inc.

No. 3:18-cv-05982-WHA (N.D. Cal. 2018)

Cybersecurity Tutorial

January 9, 2019

Presenters
Jonathan Millican, Facebook
Serrin Turner, Latham & Watkins LLP

overview

- how do attackers get access to data?
- what do attackers do with compromised data?
- how do companies defend against attacks?
- how does facebook approach security?

how do attackers get access to data?

fundamental challenges

- Physical boundaries don’t matter on the Internet
  - Attacks can come from anyone, anywhere, at any time
  - Attacker tools and techniques can easily be automated and replicated
- Vulnerabilities are inherent product of complexity
  - A codebase may contain millions of lines of code
  - Predicting and testing all potential interactions is not practically possible
- The threat landscape is highly asymmetric
  - Attacker only has to find one weakness that can be successfully exploited
  - Defender must be concerned with security of entire attack surface

online systems are complex

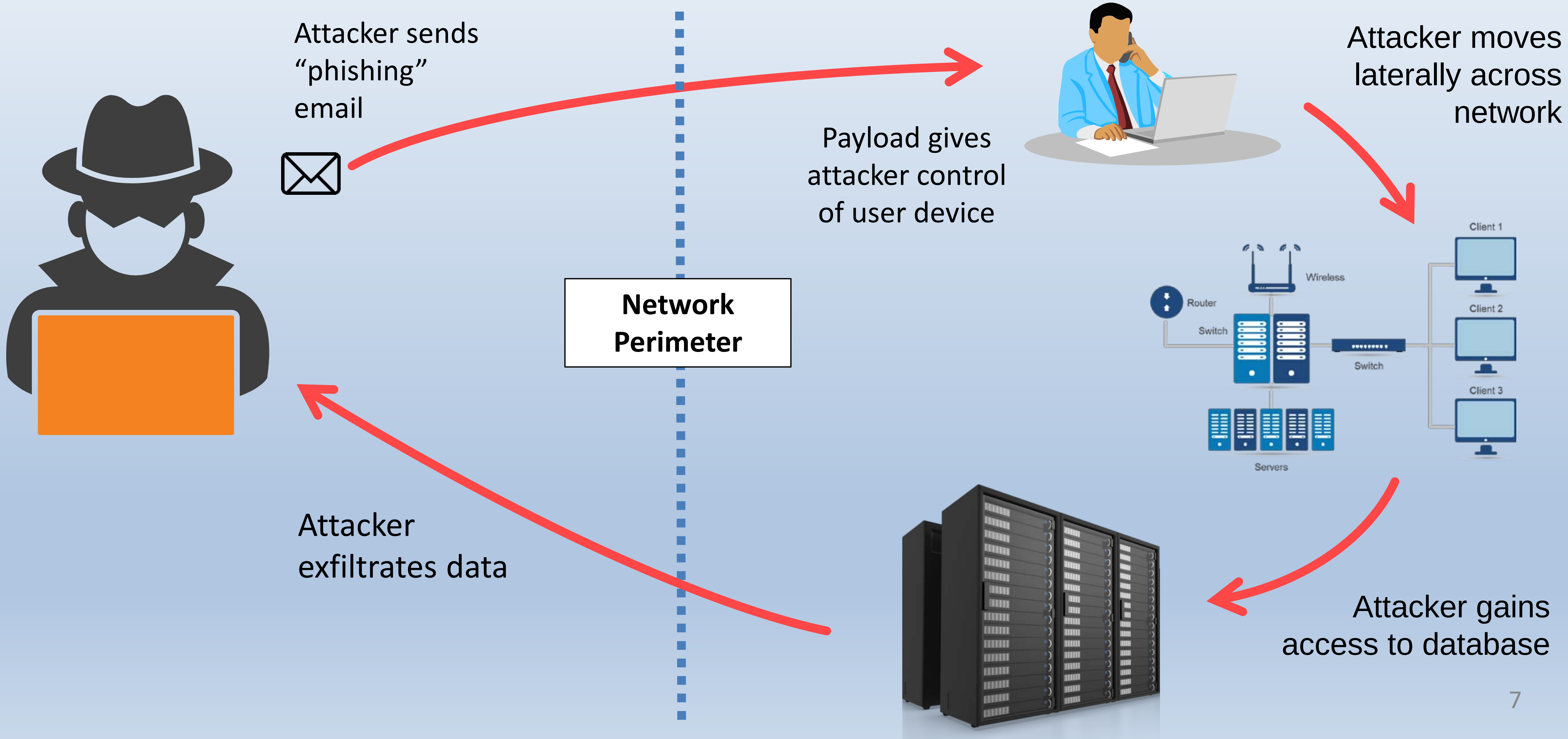
There is not one “vault door to guard”

It’s more like defending a city…

attack surface

- The attack surface consists of all points on a network potentially accessible to an external actor
  - The more complex the system, the broader the attack surface
- There are many possible vectors of attack, e.g.:
  - web-facing servers
  - user interfaces
  - developer interfaces
  - employee email
  - login portals
  - connections to third-party systems
  - and many more…

attack on internal systems



Attacker sends
“phishing”
email

Network Perimeter

Payload gives
attacker control
of user device

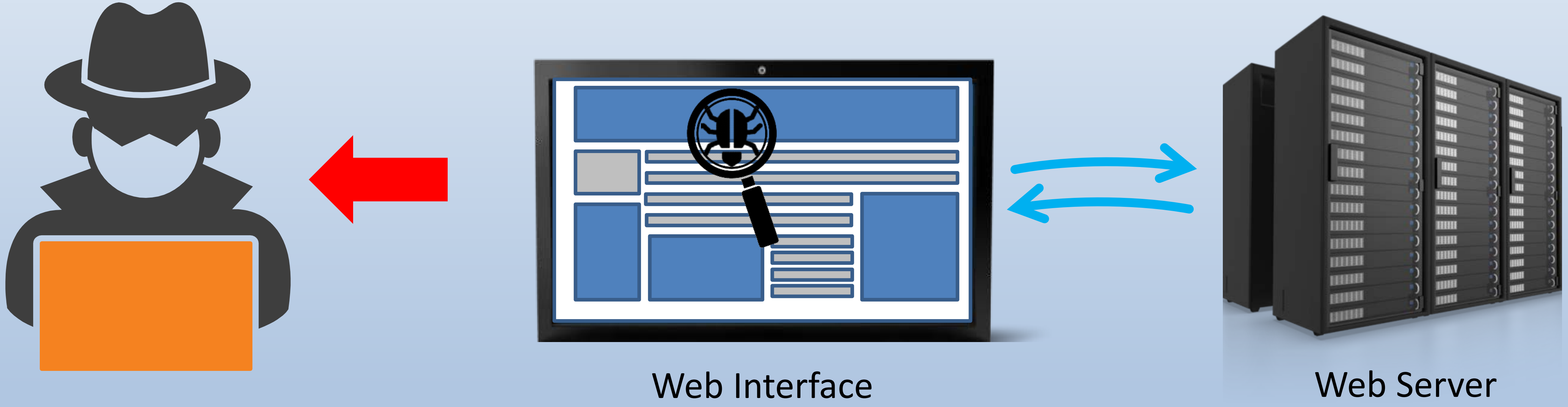
Attacker moves
laterally across
network

Attacker gains
access to database

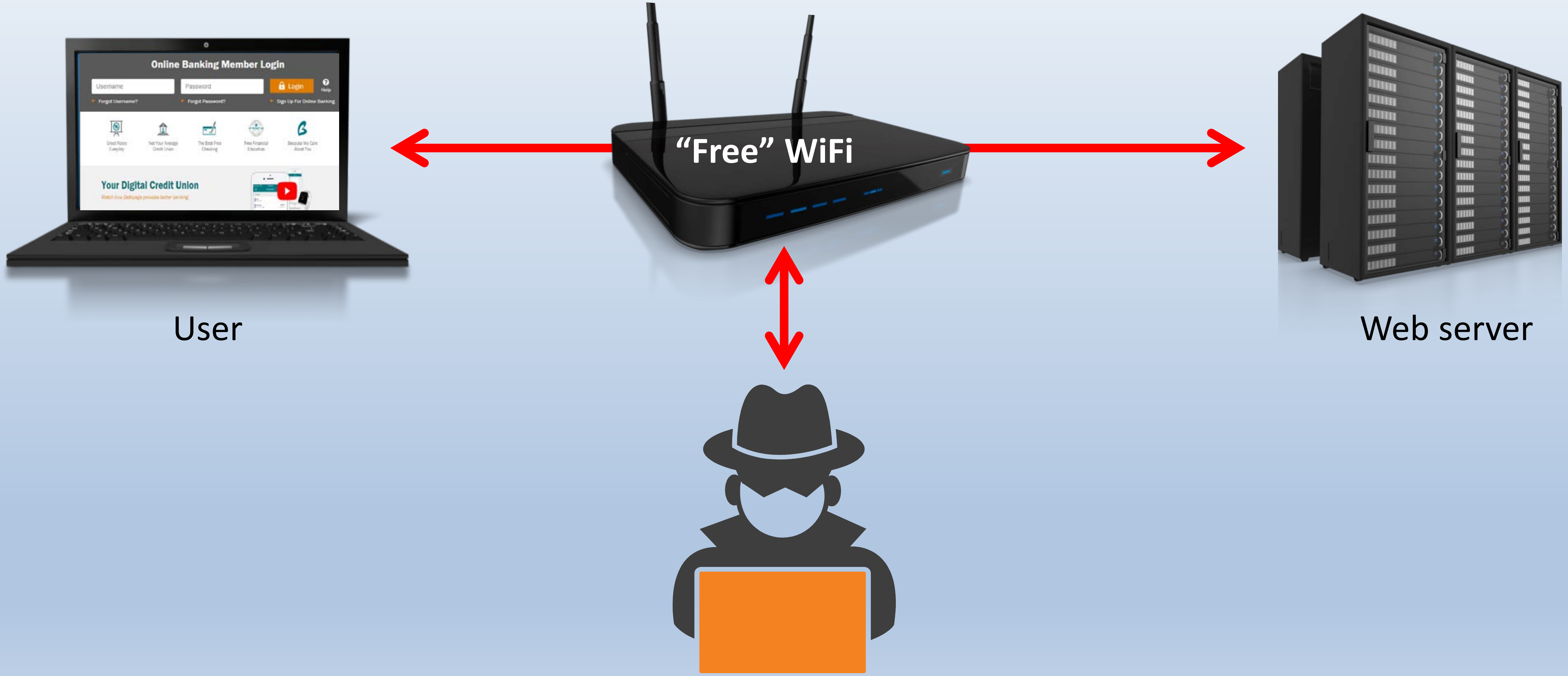
Attacker
exfiltrates data

attack on web platform

Hacker identifies bug that causes wrong data to be returned
…then exploits bug to collect exposed data



attack on transmission to user

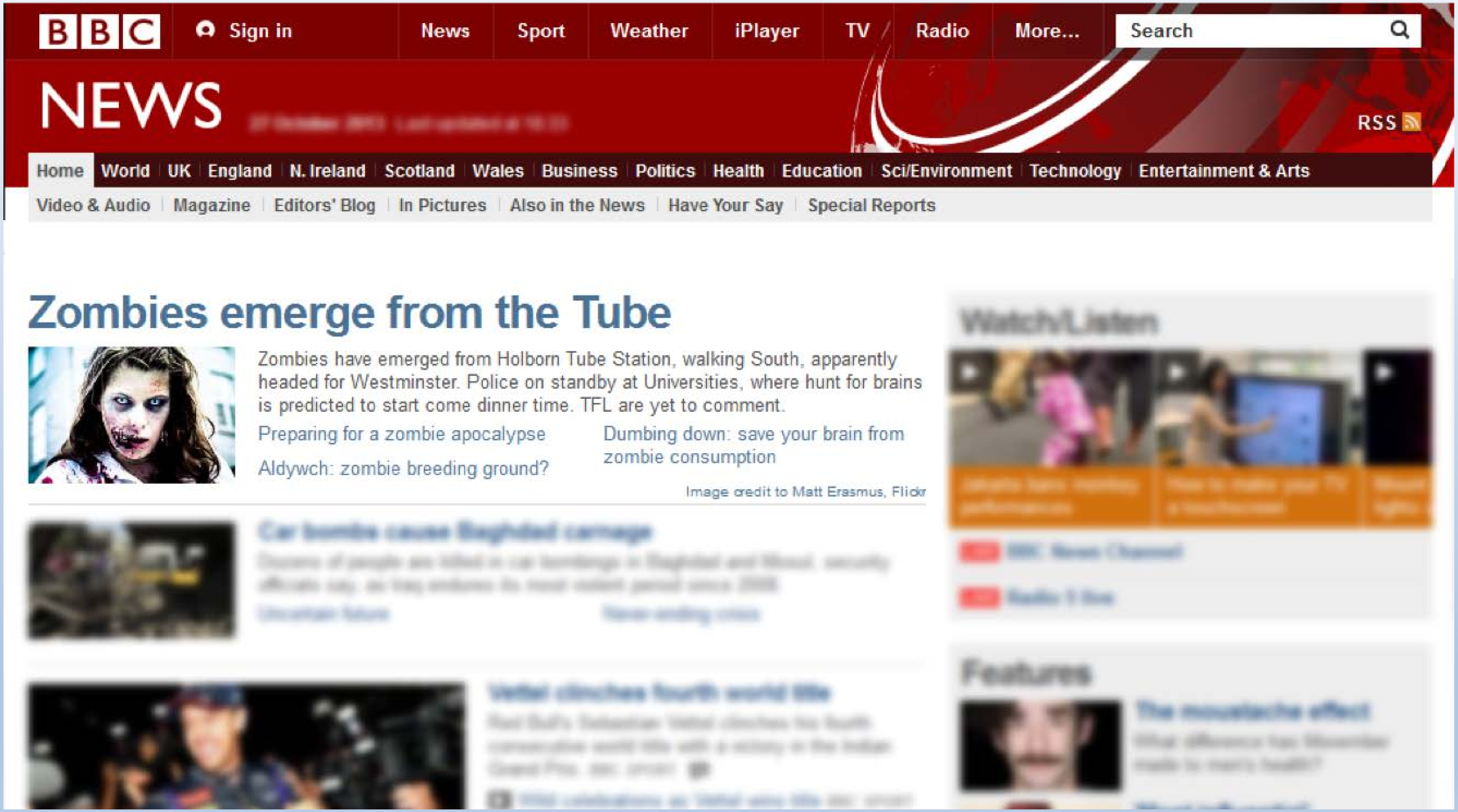


Online Banking Member Login
Username
Password
Login
Help
Forgot Username?
Forgot Password?
Sign Up For Online Banking
Your Digital Credit Union

“Free” WiFi

User

Web server



Zombies emerge from the Tube

Zombies have emerged from Holborn Tube Station, walking South, apparently headed for Westminster. Police on standby at Universities, where hunt for brains is predicted to start come dinner time. TFL are yet to comment.

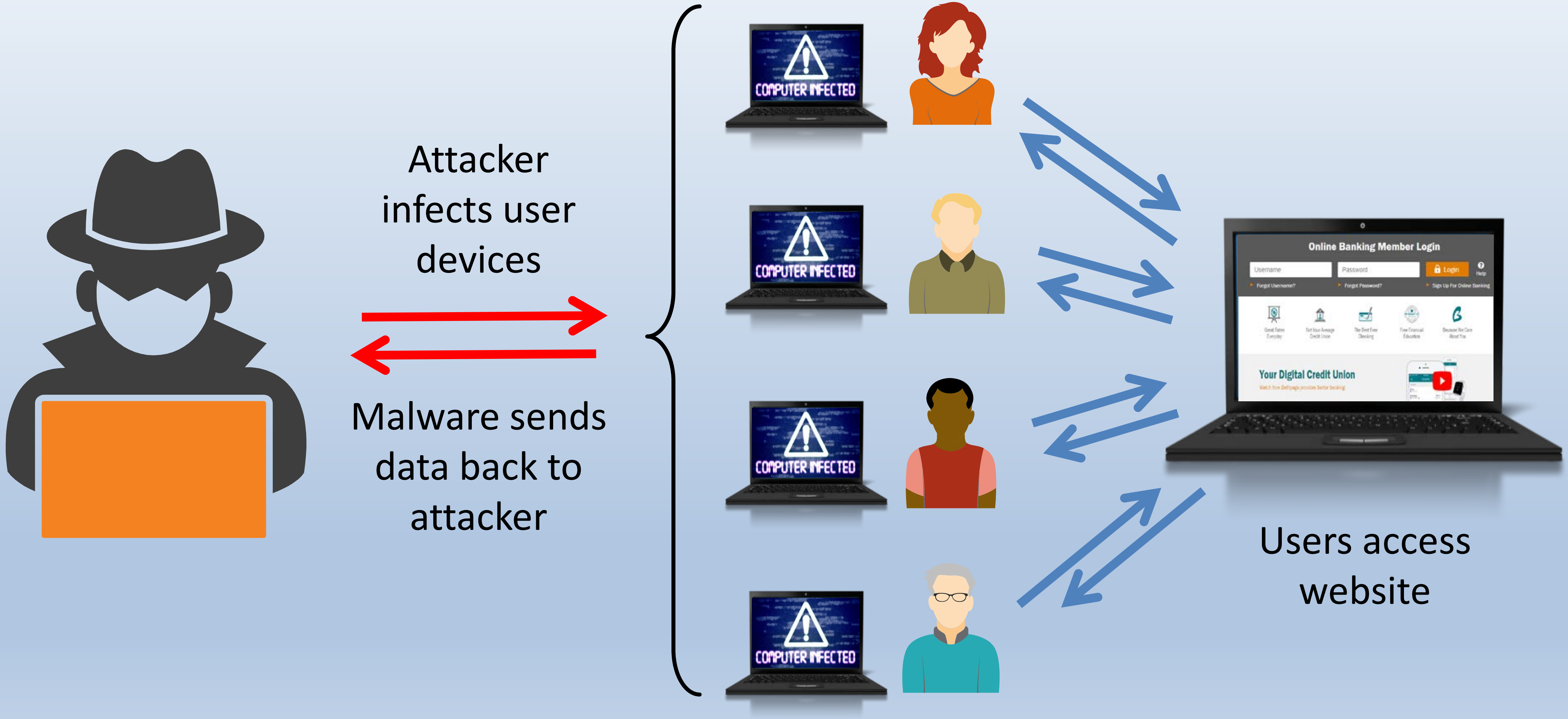
Preparing for a zombie apocalypse

Aldywch: zombie breeding ground?

Dumbing down: save your brain from zombie consumption

Image credit to Matt Erasmus, Flickr

attack on user devices



Attacker infects user devices

Malware sends data back to attacker

Users access website

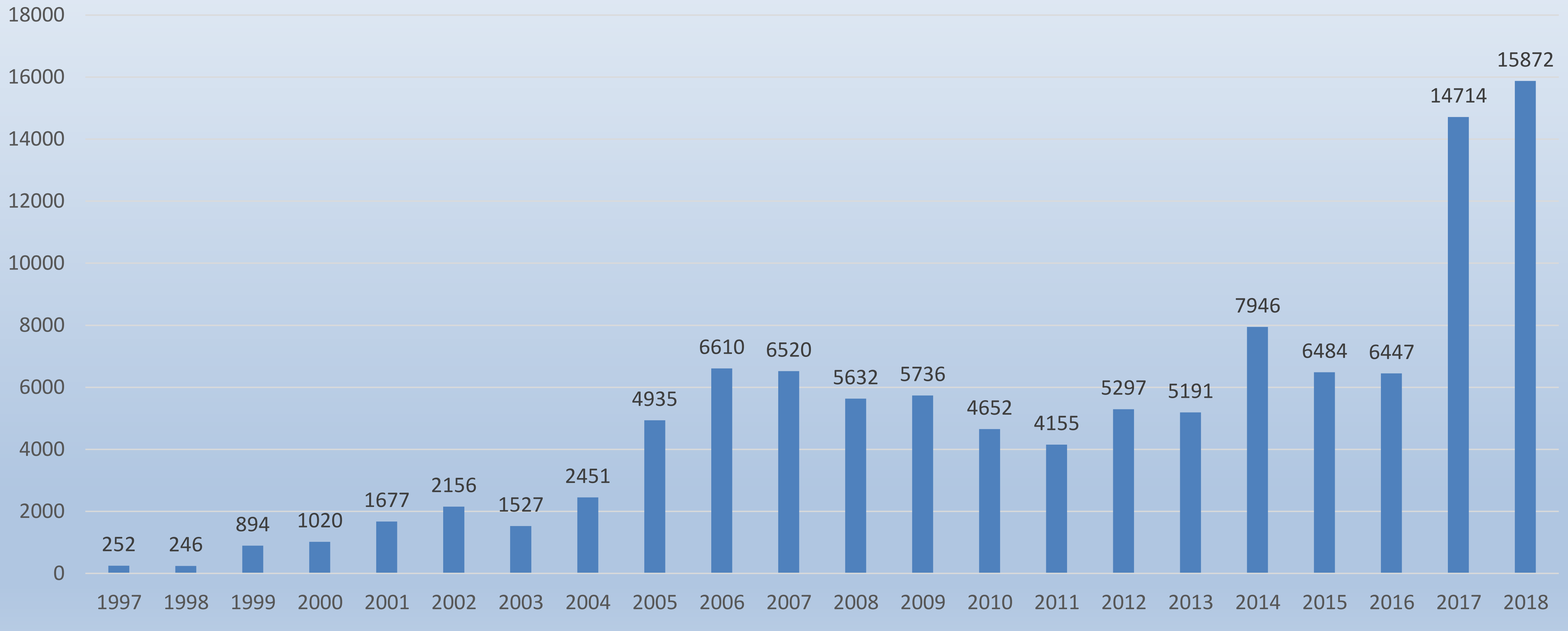
vulnerabilities

- Attacks often involve, at some level, the exploitation of a software vulnerability

- Most of these attacks exploit failures to patch ***publicly known*** vulnerabilities in third-party software

- Thousands of such common vulnerabilities and exposures (CVEs) are reported every year

publicly reported vulnerabilities



***MITRE CVE Website*, cve.mitre.org**

“zero-day” vulnerabilities

- More rarely, an attack may exploit a “zero-day” vulnerability
  - i.e., a vulnerability unknown before it is used in an attack, which the software developer has had “zero days” to fix
- Zero-day vulnerabilities often require sophistication to identify
  - But less sophisticated actors may be able to buy exploits for them through criminal networks

what do attackers do with compromised data?

threat actors

Different threat actors have different objectives

Nation-states

- Espionage
- Political interference
- Sabotage

Criminals

- Identity theft/fraud
- Extortion
- Spamming

Hacktivists

- Disruption
- Leaking/doxing
- Ideological protests

Competitors/Insiders

- IP theft
- Commercial advantage
- Diversion of business

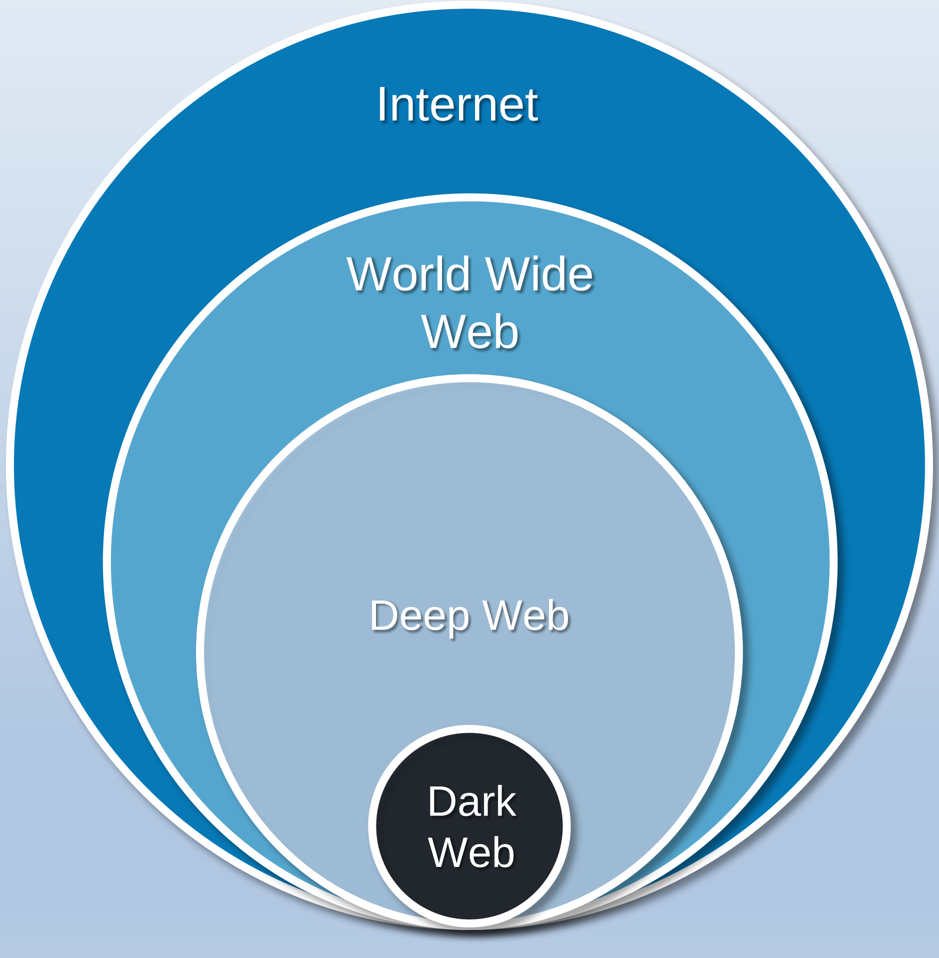
identity theft

- Many attackers seek to steal data that can be used to commit identity theft and financial fraud
  - e.g., SSNs, credit card numbers, payment account credentials, bank account information
- The data can then be sold to identity thieves through black markets on the “dark web”

“deep web” vs. “dark web”

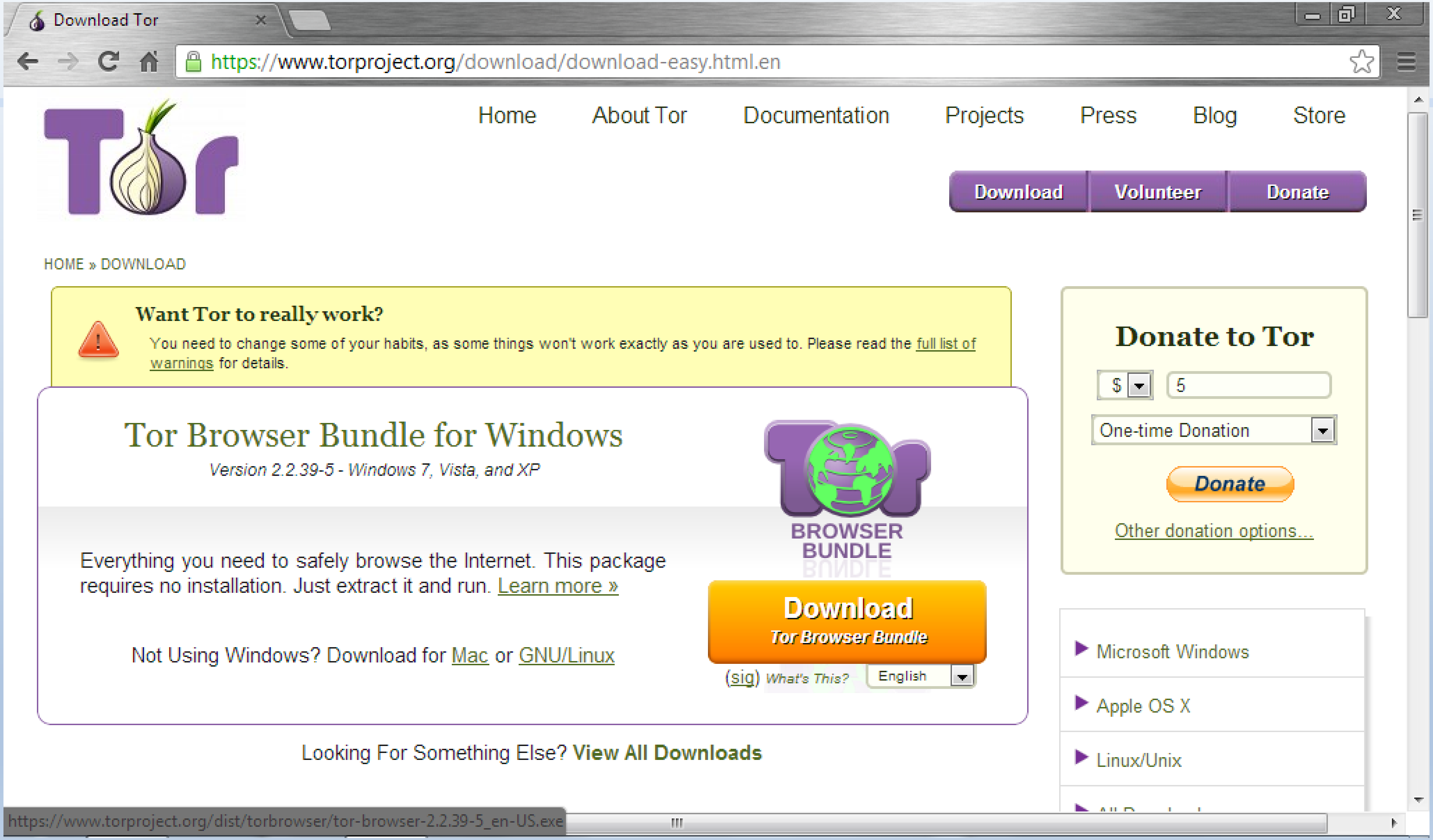
- Much of the content on the internet is not indexed on search engines and is known as the “**deep web**”

- The “**dark web**” refers to websites whose IP addresses are hidden using specialized technologies (such as the Tor network)



criminal activity on the dark web

- Many criminal websites operate on the dark web to evade the reach of law enforcement
  - concealment of true IP addresses makes it difficult for law enforcement to seize or shut down servers
- Examples include: dark markets, carding sites, black-hat hacking forums



HOME » DOWNLOAD

Want Tor to really work?

You need to change some of your habits, as some things won't work exactly as you are used to. Please read the full list of warnings for details.

Tor Browser Bundle for Windows

Version 2.2.39-5 - Windows 7, Vista, and XP

Everything you need to safely browse the Internet. This package requires no installation. Just extract it and run. Learn more »

Not Using Windows? Download for Mac or GNU/Linux

(sig) *What's This?*

Looking For Something Else? **View All Downloads**

Donate to Tor

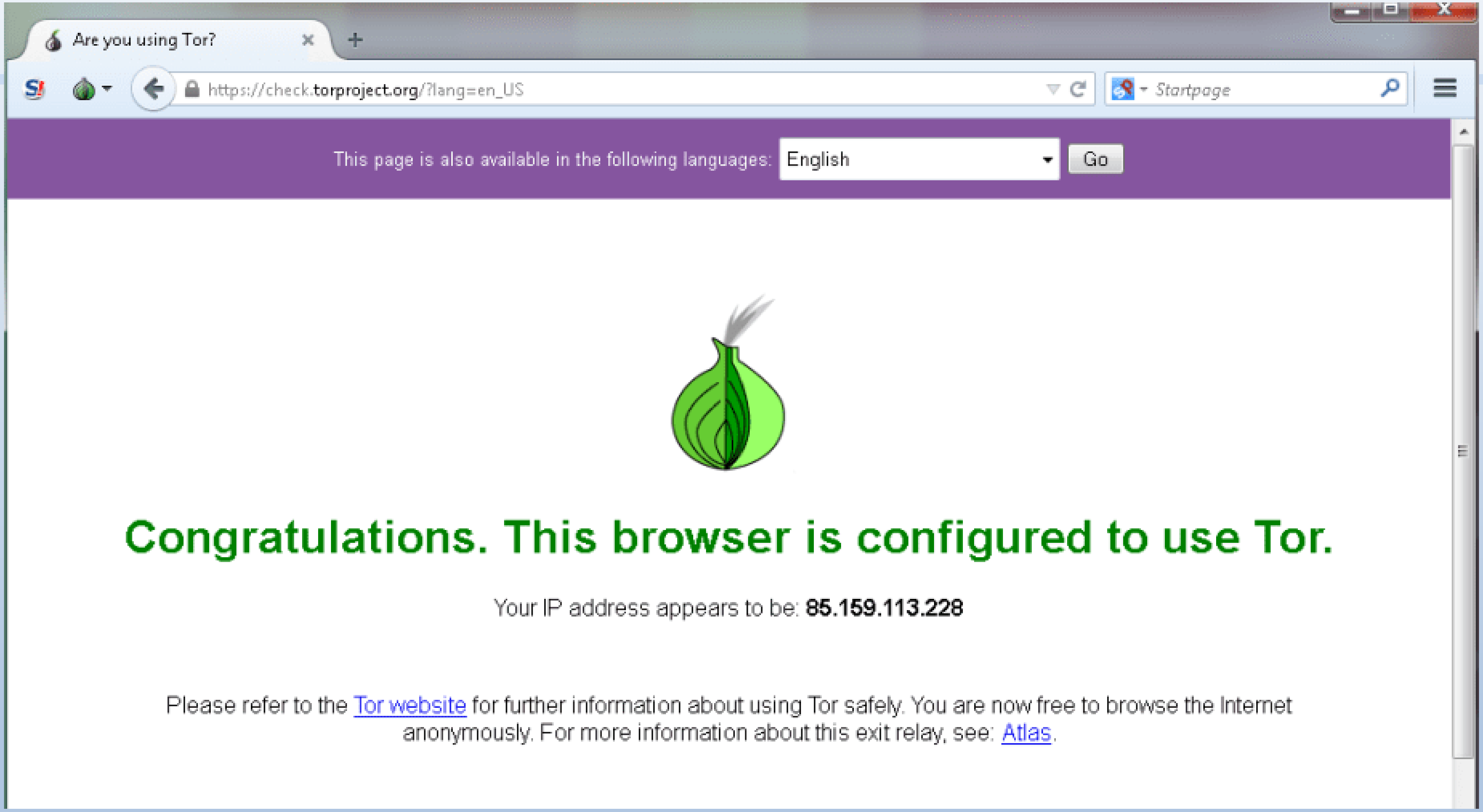
$ 5

One-time Donation

Donate

Other donation options...

https://www.torproject.org/dist/torbrowser/tor-browser-2.2.39-5_en-US.exe



This page is also available in the following languages: English

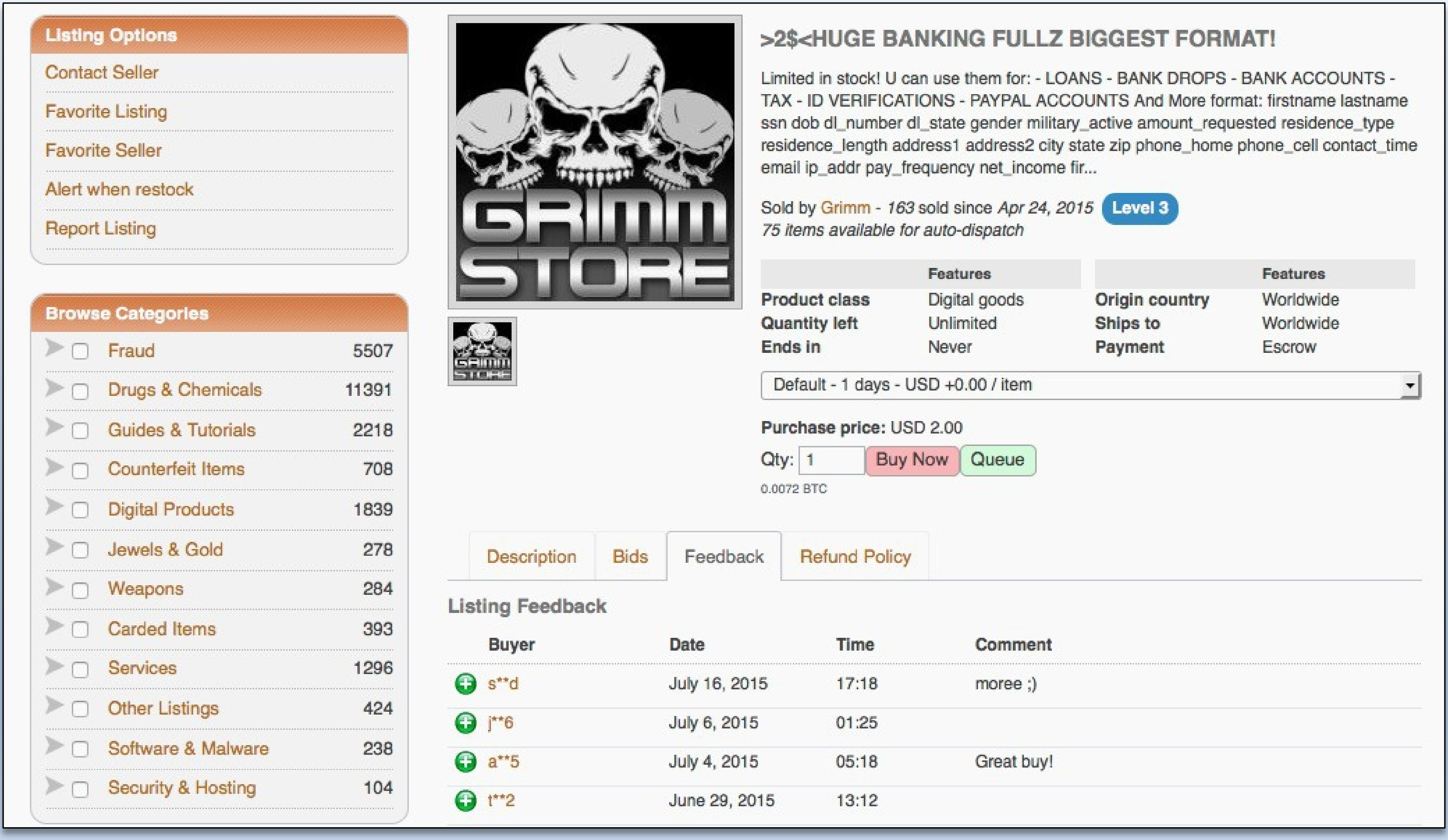
Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **85.159.113.228**

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: Atlas.

Your IP address appears to be: **85.159.113.228**

example: banking information sold on “Alpha Bay” market



Listing Options

- Contact Seller
- Favorite Listing
- Favorite Seller
- Alert when restock
- Report Listing

Browse Categories

□	Fraud	5507
□	Drugs & Chemicals	11391
□	Guides & Tutorials	2218
□	Counterfeit Items	708
□	Digital Products	1839
□	Jewels & Gold	278
□	Weapons	284
□	Carded Items	393
□	Services	1296
□	Other Listings	424
□	Software & Malware	238
□	Security & Hosting	104

>2$<HUGE BANKING FULLZ BIGGEST FORMAT!

Limited in stock! U can use them for: - LOANS - BANK DROPS - BANK ACCOUNTS - TAX - ID VERIFICATIONS - PAYPAL ACCOUNTS And More format: firstname lastname ssn dob dl_number dl_state gender military_active amount_requested residence_type residence_length address1 address2 city state zip phone_home phone_cell contact_time email ip_addr pay_frequency net_income fir...

Sold by Grimm - *163* sold since *Apr 24, 2015* Level 3
75 items available for auto-dispatch

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 2.00

Qty: 1 Buy Now Queue

0.0072 BTC

Description | Bids | Feedback | Refund Policy

Listing Feedback

Buyer	Date	Time	Comment
s**d	July 16, 2015	17:18	moree ;)
j**6	July 6, 2015	01:25	
a**5	July 4, 2015	05:18	Great buy!
t**2	June 29, 2015	13:12	

spamming

- Not all data is sought (or useful) for identity theft
  - E.g., some major data thefts have involved only names and email addresses
- Spammers seek contact and marketing data to target their solicitation activity
  - Such data may not be illicit on its face and may end up sold on the ordinary (“surface”) web

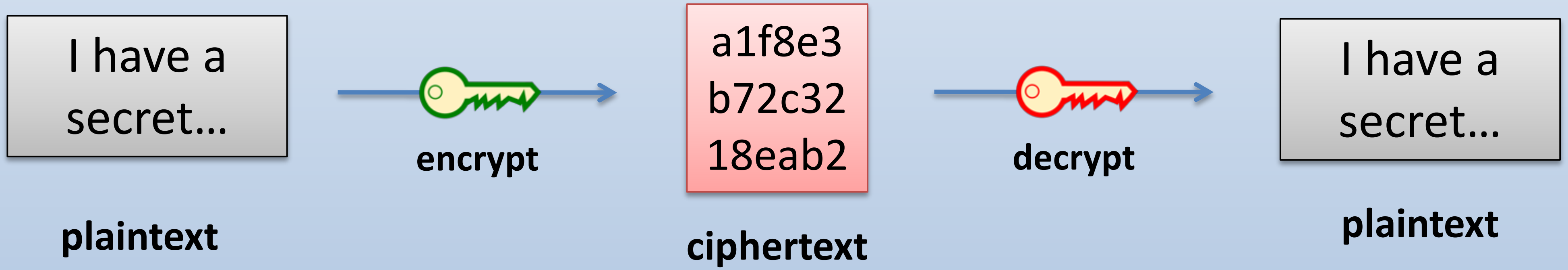
how do companies defend against attacks?

no “magic bullet” solutions

- There is no simple answer to the question of how companies protect user information
- Security cannot be guaranteed by any single product or technology
- Each individual security measure is only effective against a limited set of risks
  - Encryption provides an example of this principle

encryption

- Encryption is the encoding of data so that it can only be read by those who have the necessary "key"



I have a secret…

plaintext

encrypt

a1f8e3
b72c32
18eab2

ciphertext

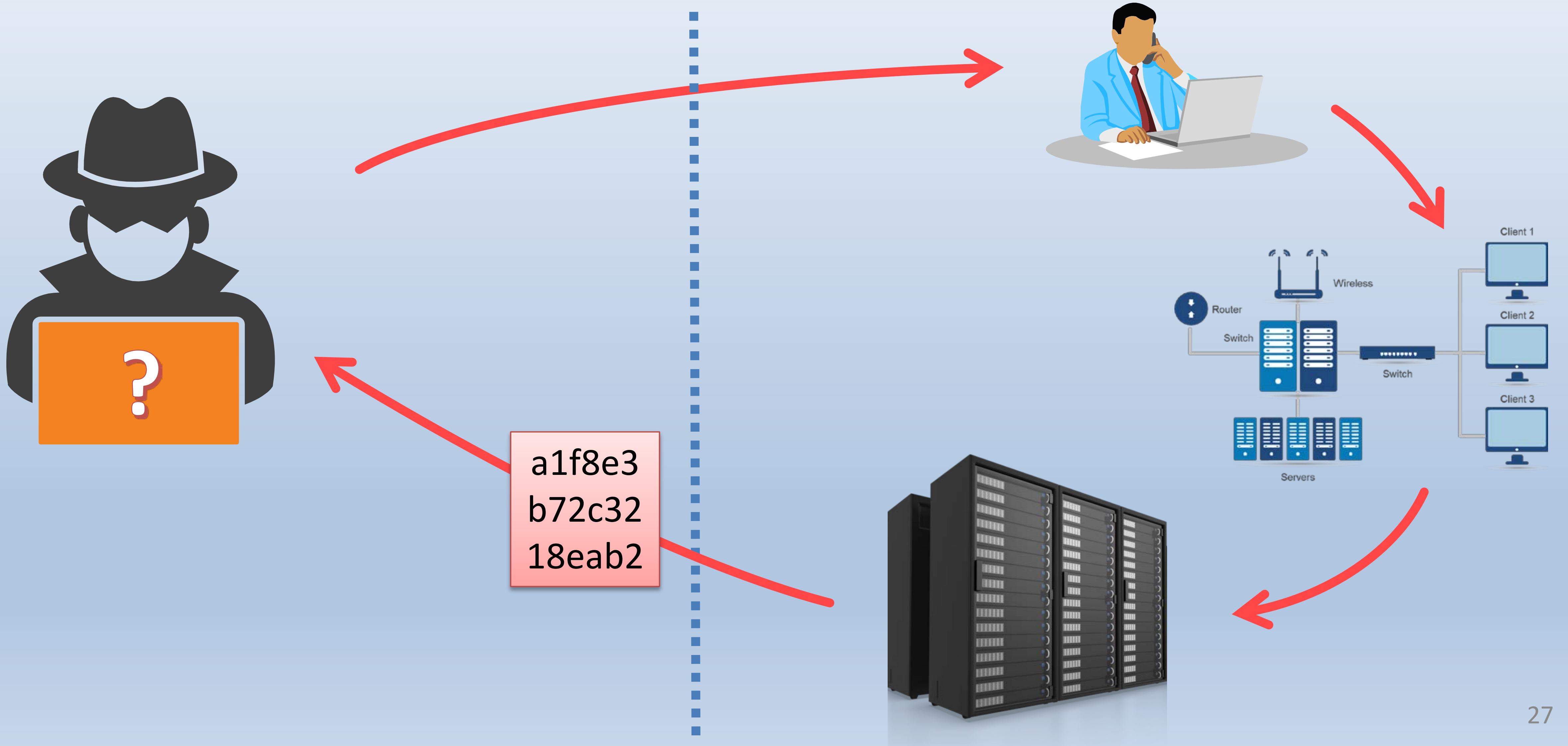
decrypt

I have a secret…

plaintext

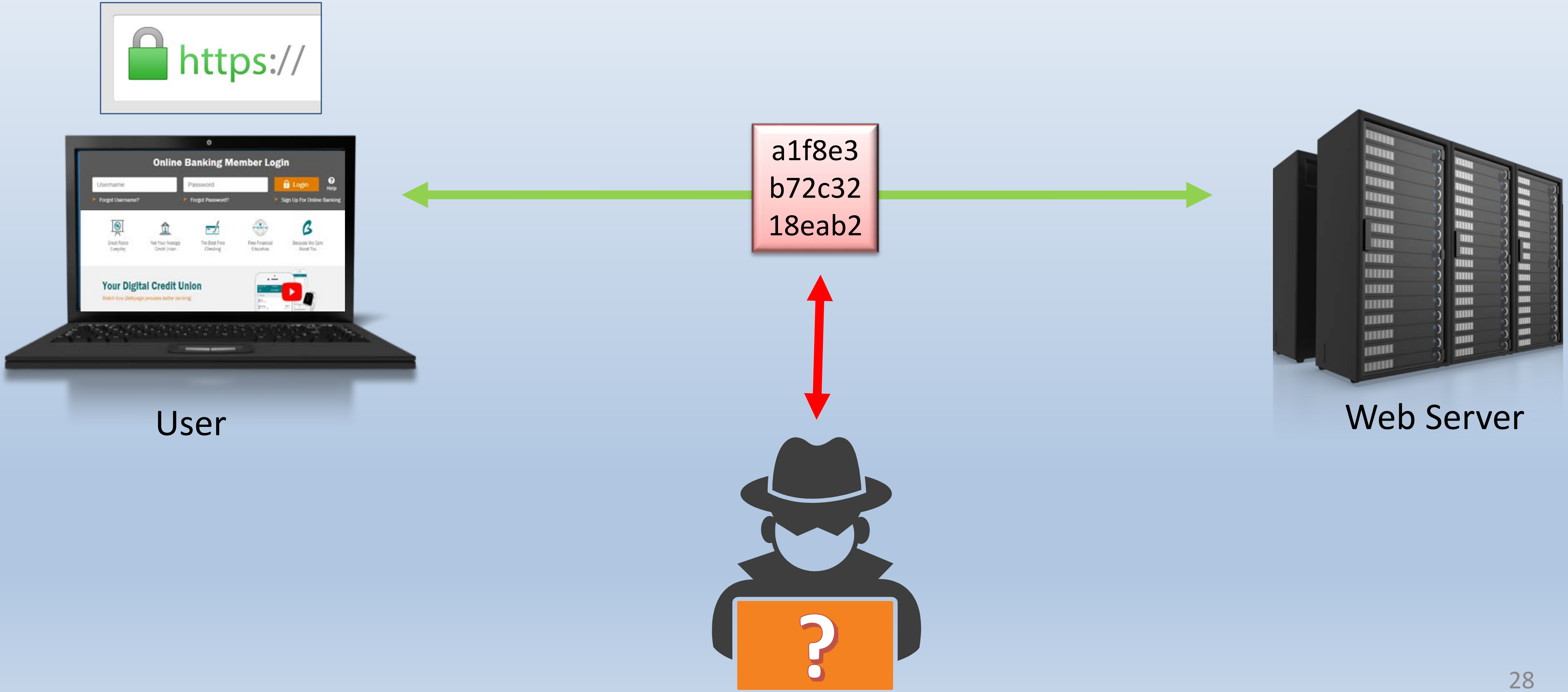
- Encryption is an important security control in specific contexts but does not protect against certain forms of attack

encryption of data at rest



a1f8e3
b72c32
18eab2

encryption of data in transit


https://
Online Banking Member Login
Username
Password
Login
Help
Forgot Username?
Forgot Password?
Sign Up For Online Banking
Your Digital Credit Union
?

a1f8e3
b72c32
18eab2

User

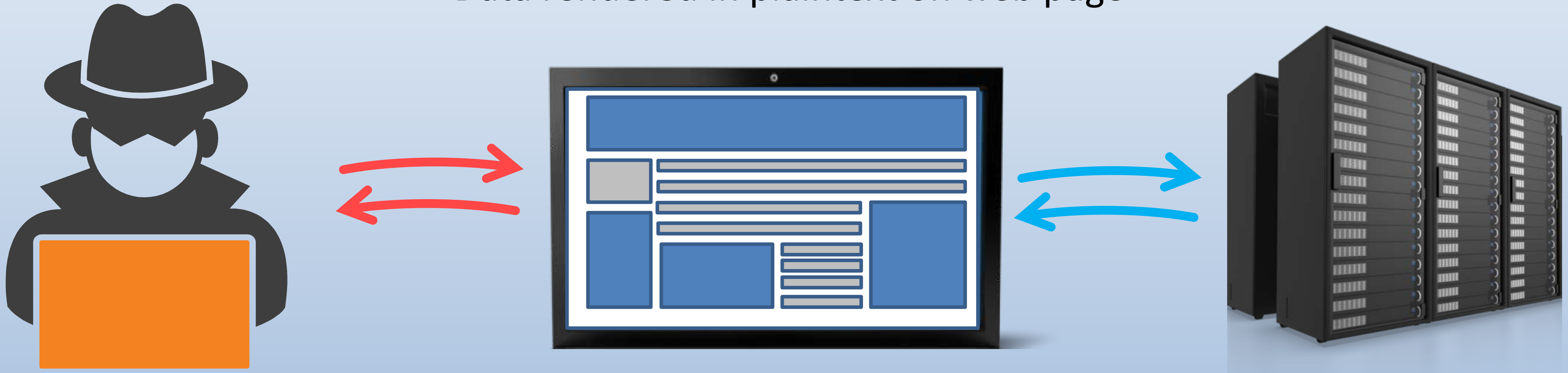
Web Server

limitations of encryption

- In various contexts, data must be accessible in plaintext in order to be useful
  - e.g., users must be able to see their own data
- In such contexts, encryption may not be a relevant control
  - e.g., if attackers are able to access a user’s account, they can access data meant to be visible from account

limitations of encryption

Data rendered in plaintext on web page



Web Interface

Web Server

information security program

- What is true for encryption is true generally:
  no single control provides a complete solution

- A comprehensive security program instead relies on a broad range of controls addressed to a broad range of risks

information security program

While any security program must be tailored to a company's unique risk profile, typical components include:

- firewalls
- network segmentation
- vulnerability management
- penetration testing
- logging and monitoring
- encryption
- secure product development

- threat intelligence
- identity management
- permissions management
- vendor management
- data deletion
- physical security
- incident response

risk-based approach

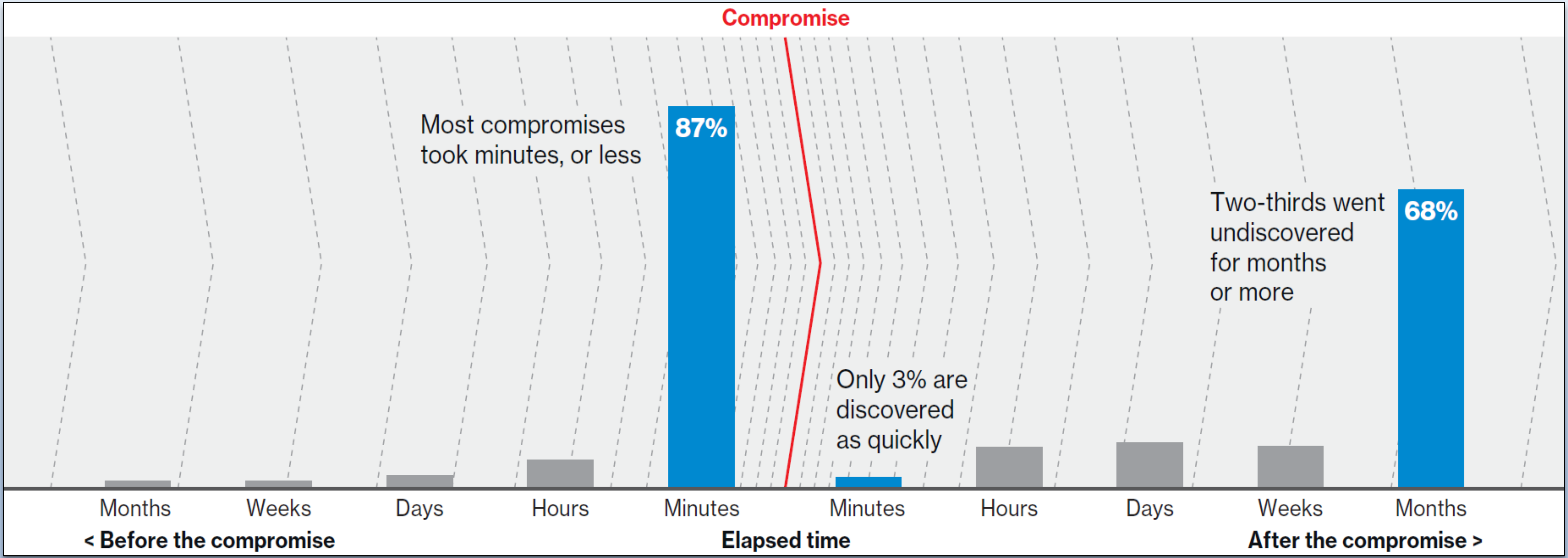
- There is no single checklist or set of rules that a company must or should follow
  - Systems and threats widely vary and evolve
  - Tick-box approach leaves many gaps
- Effective security requires a **risk-based** approach
  - Resources must be allocated by risk level
  - Security must be balanced against functionality

incident detection & response

- Because some attacks may not be prevented, detection and response are important components of security

- Both components present challenges
  - Attacker activity may be difficult to recognize or distinguish from legitimate activity
  - Scope, cause, and remediation of attack require time to investigate and analyze

detection time



Source: 2018 Verizon Data Breach Investigations Report

how does facebook approach security?

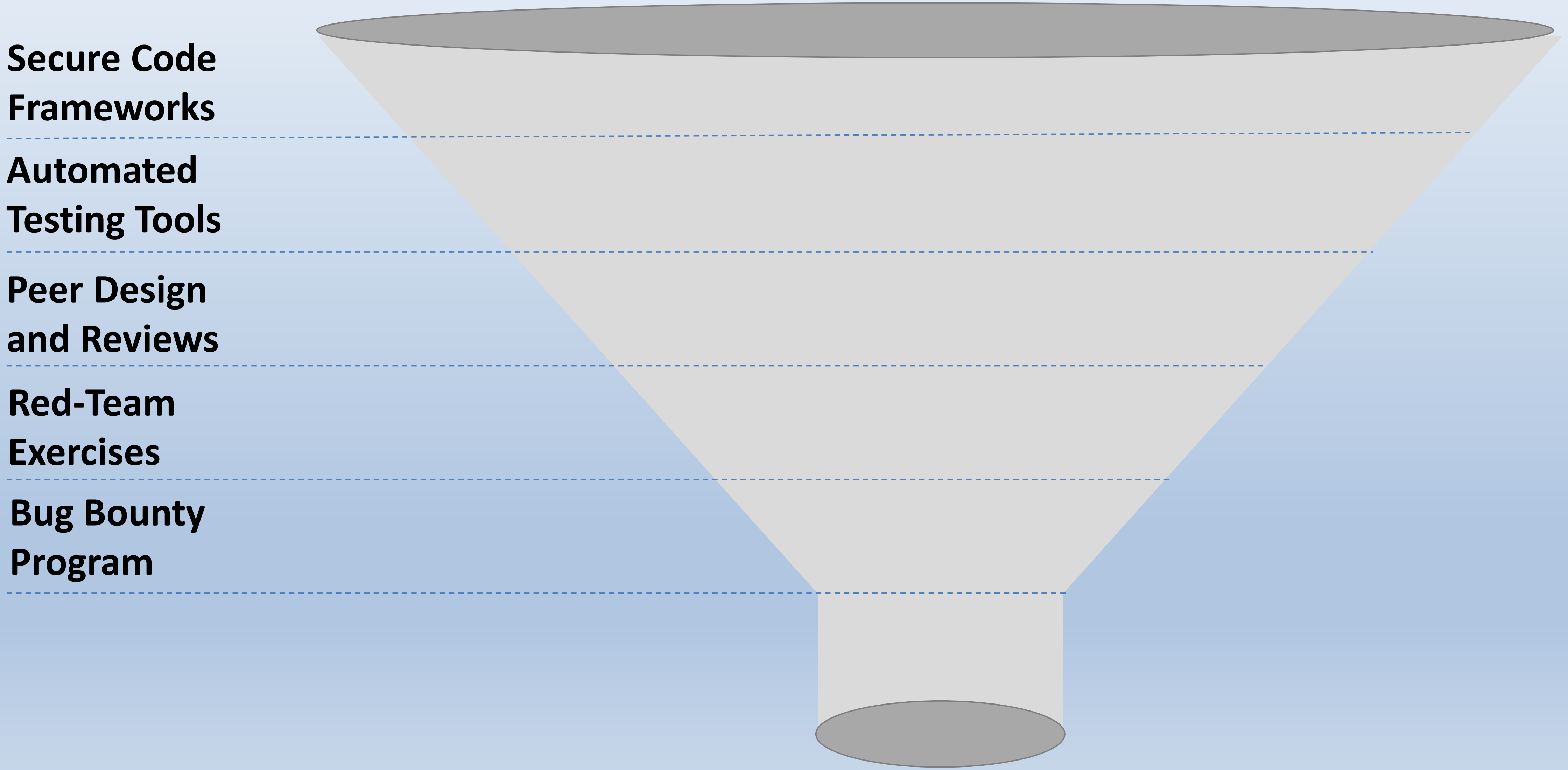
security by design

- We design systems to incorporate security principles and lessons-learned directly into the software development process
  - We work to make our code libraries and frameworks secure by default
  - The goal is to make the easiest way to write code the safe way

defense in depth

- Our goal is to maximize the number of hurdles that must be overcome for a vulnerability to exist or be exploited
- Each individual layer of security may miss things, but together they make it very difficult for an attacker to find and exploit a weakness

layers of security



Secure Code Frameworks

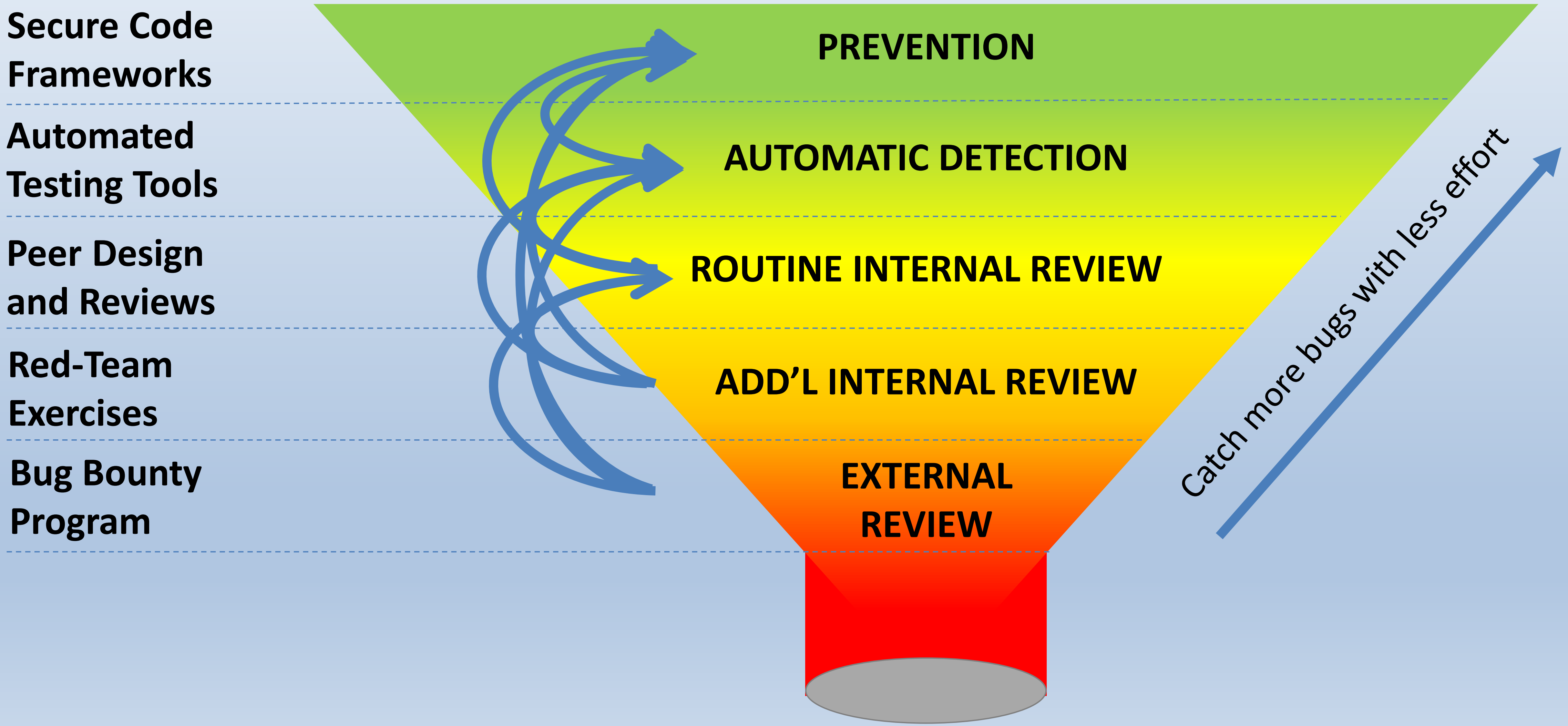
Automated Testing Tools

Peer Design and Reviews

Red-Team Exercises

Bug Bounty Program

security is an iterative process



Secure Code Frameworks

Automated Testing Tools

Peer Design and Reviews

Red-Team Exercises

Bug Bounty Program

security innovation

- We have built industry-leading technologies as part of our security program
  - These include tools for preventing and detecting potential vulnerabilities (e.g., Zoncalan, Invariant Detector)
- We release our tools as open-source software where possible (e.g., Infer, Hack, XHP, OSQuery)
  - Other prominent technology companies have adopted these tools for their own use

summary

summary

- There are many different vectors and types of attack
  - Zero-day vulnerabilities are the most challenging to defend
- Attackers widely vary in their motives and objectives
  - Not all hackers seek information for identity theft
- Companies cannot equally defend against every threat
  - A risk-based approach is required
- Facebook leverages many layers of defense
  - Security-by-design is built into the coding process