Chapter 23

The Bleeding Edge

Omer Green

Introduction

- We have become dependent on a variety of vulnerable online applications
- Developers usually don't care until they get hacked
- In this lecture we will discuss 3 applications which make up the bleeding edge of security research

Lecture Contents

- Computer Games
- Web Applications
- Privacy Technology

Computer Games

- Games were one of the first computer applications
- The game development industry has grown in the last decades
- Some people will try to cheat, especially in multiplayer games
- We will discuss cheating in online games

Credit: Riot Games

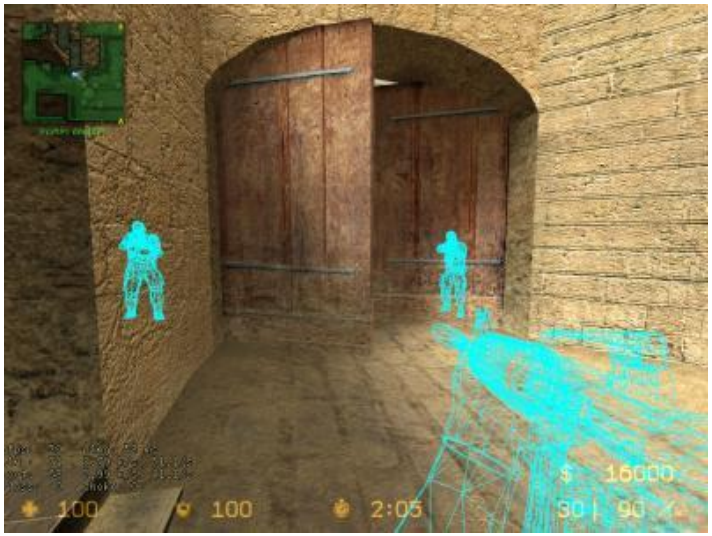
Cheating

- There are 3 types of cheating:
  - Exploiting vulnerabilities that existed in an offline game and made it into the online world
  - Applying known computer-security issues to the game
  - New cheating tactics that emerge because of the nature of online computer games

Unauthorized software

- A popular cheating strategy is to run your own programs – bots
- Those bots come in a variety of sophistication levels
- The developers try to prevent that by encrypting the packet stream and using antivirus-like guard software

Credit: hackerbot.net



Credit: wallhack.blog.hu

Virtual Economies

- Bots are used for farming in multiplayer games
- As people buy the farmed goods with money, macroeconomic effects start to matter
- Exchange rates, illegal gambling

Credit: Google images

- In EVE Online a single high-end ship can cost thousands of dollars.
- A player's misclick can ignite wars that cost tens or even hundreds of thousands of real dollars.

Credit: CCP Games

Web Applications

- More and more services are accessible through web browsers
- There are many common problems to all kinds of websites:
  - Not sanitizing input
  - Exposure of the inner structure of the website
- Securing websites is especially important nowadays

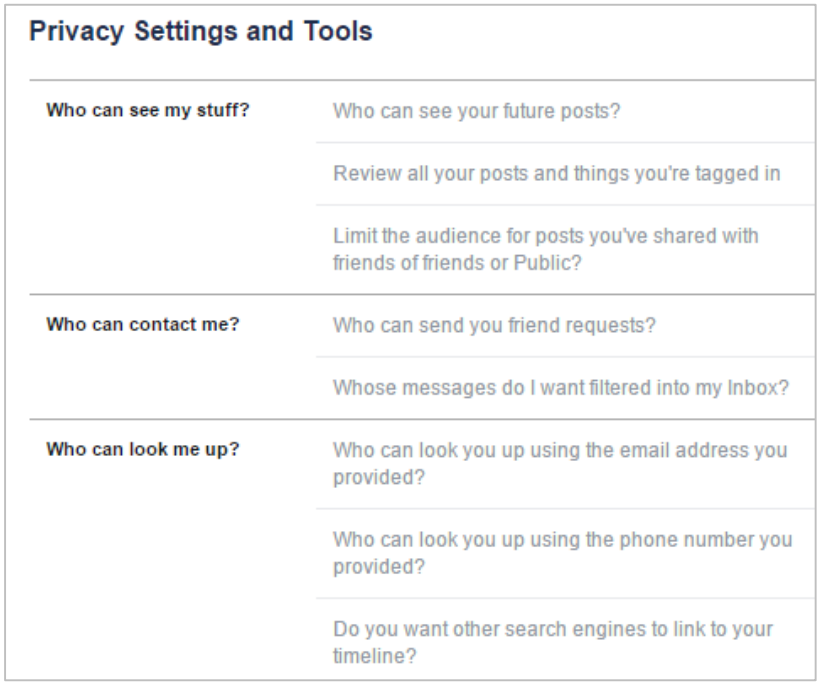
Social Networking Websites

- Social Networking Websites have taken off rapidly since 2004
- Peer pressure – everyone has a Facebook account
- Holds massive amount of personal information – excellent targeted advertisement

Credit: thoughtpurusits.com

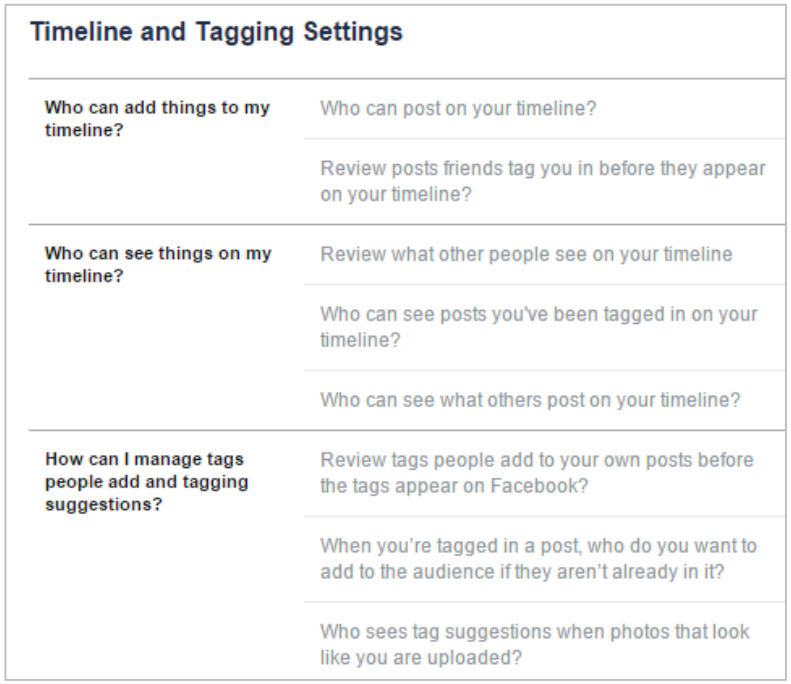
Social Networking Websites

- Access control is very important in these websites
- The security policy is very complex



Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?
	Review all your posts and things you're tagged in
	Limit the audience for posts you've shared with friends of friends or Public?
Who can contact me?	Who can send you friend requests?
	Whose messages do I want filtered into my Inbox?
Who can look me up?	Who can look you up using the email address you provided?
	Who can look you up using the phone number you provided?
	Do you want other search engines to link to your timeline?



Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?
	Review posts friends tag you in before they appear on your timeline?
Who can see things on my timeline?	Review what other people see on your timeline
	Who can see posts you've been tagged in on your timeline?
	Who can see what others post on your timeline?
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?
	Who sees tag suggestions when photos that look like you are uploaded?

Credit: facebook.com

Social Networking Websites

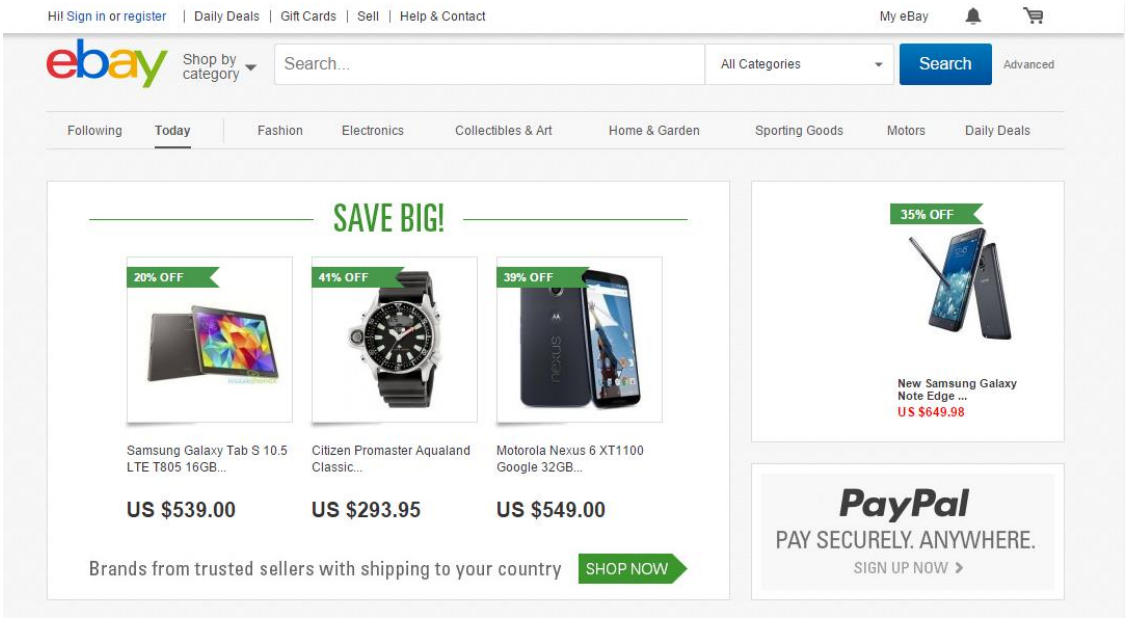
- There are subtle policy issues
  - Notifying your status changes to your friends
  - Using private information in searches
  - Authorizing third-party applications
- Facebook leaves the hard security decisions to the users
- Dealing with social issues
  - Bullying
  - Internet lynching/Social Shaming

Social Networking Websites

- Before the industrial revolution, most people lived in villages – zero privacy
- Moving to towns gave people anonymity
- Now the world is steadily becoming more documented and people have less privacy, again
- Despite all the issues, social network websites have their perks

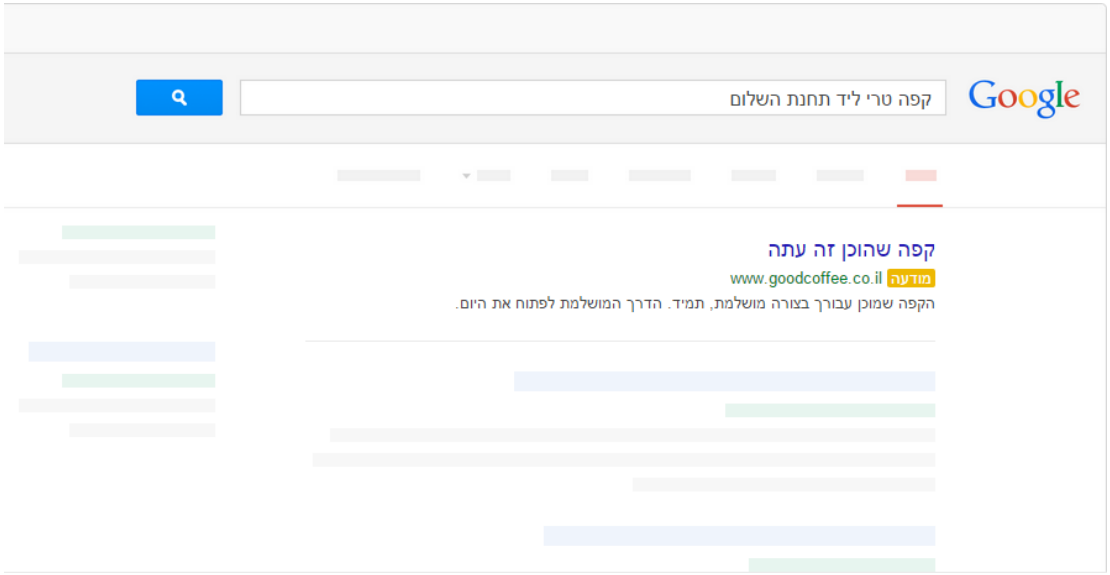
eBay

- The largest target for phishing, along with PayPal
- Has both new and old-fashioned fraud
- Uses a reputation system that can be exploited



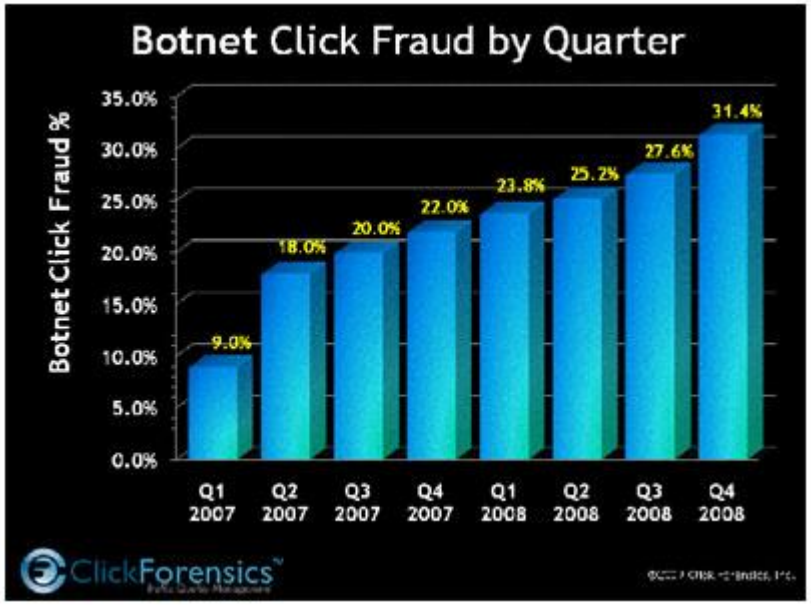
Google

- Google uses the Pagerank algorithm
- Gets revenue by placing personalized ads (AdWords)
- Website owners can display relevant ads and get paid (AdSense)



Google

- AdWords & AdSense proved to be hugely popular and profitable, but (as you might guessed) were prone to exploits:
  - Click-fraud
  - Impression spam
  - Google arbitrage
  - Made-for-AdSense websites
- Google Hacking – using Google to find vulnerable targets



Privacy Technology

- Technology is putting social conventions under strain
  - Denying past conversations
  - Anonymity

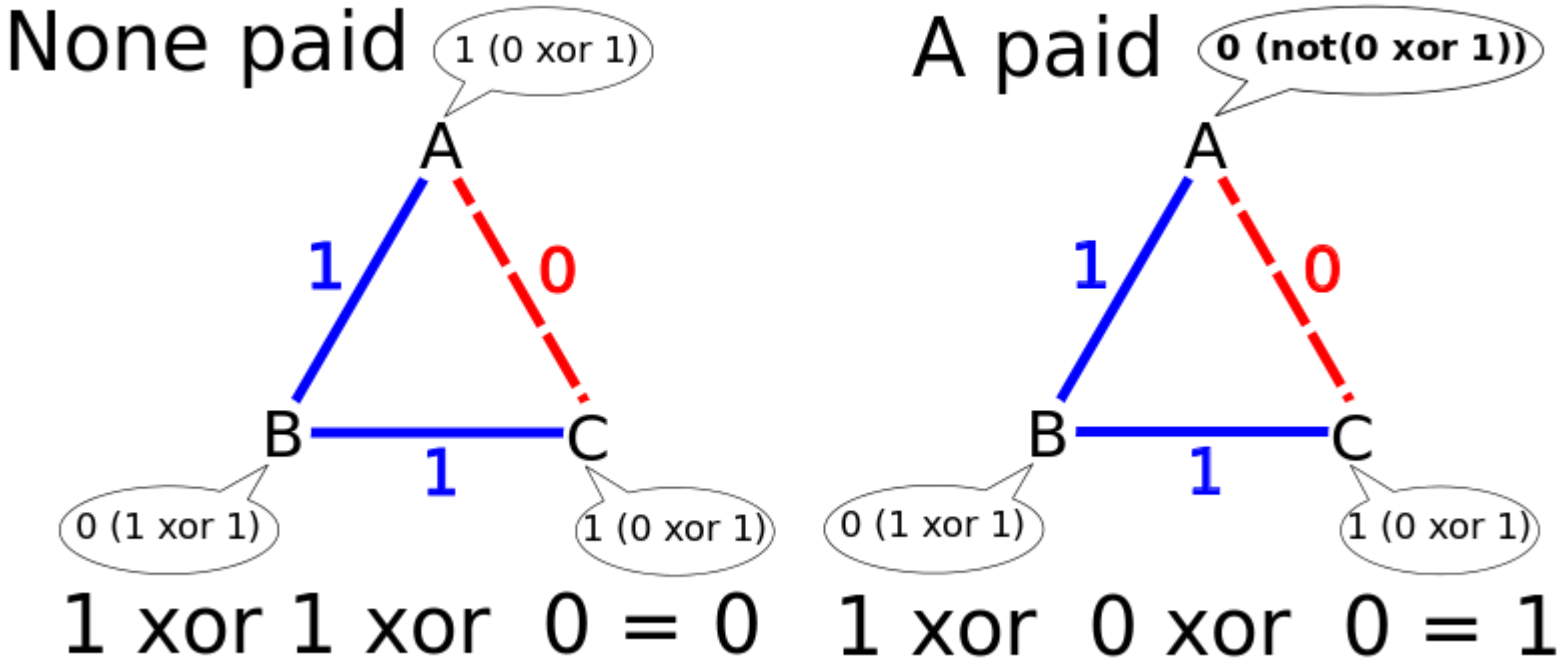
Anonymous Email

- Even if the communication is encrypted, the fact that it happened may give the game away
- The dining cryptographers problem
- For practical applications - anonymous remailer

$$A \rightarrow C: \{D, \{B, \{M\}_{KB}\}_{KD}\}_{KC}$$

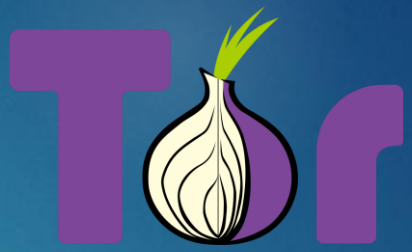
- Intelligence agencies can operate remailers as honey traps

Dining Cryptographers



Credit: Wikipedia.org

Tor



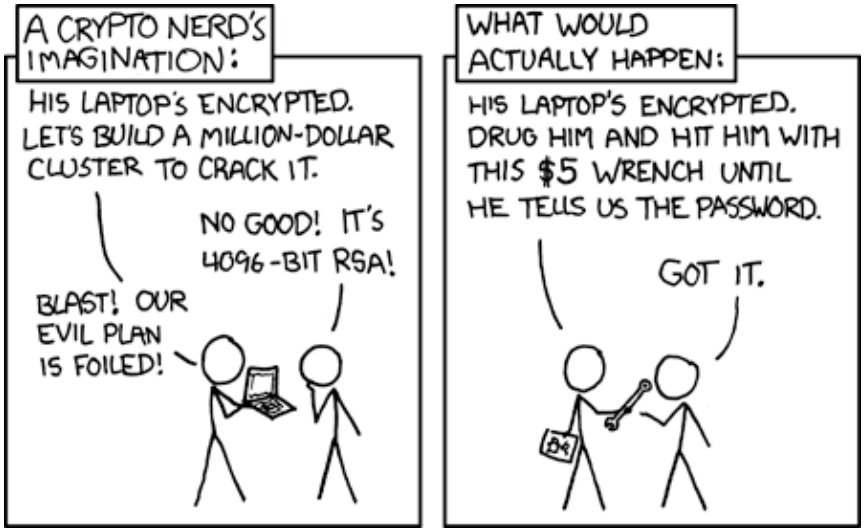
- The Onion Router – system for anonymous communication and web browsing
- Uses onion routing
- Vulnerabilities:
  - End-to-end communication is not encrypted
  - Malicious exit node
  - Side channels
  - Exposed to traffic analysis by capable adversaries
  - Applications can get user to identify themselves explicitly and implicitly
  - Traffic patterns can still give you away

Email Encryption

- PGP

$$\{KS\}_{KB}, \{M, \{h(M)\}_{KA}^{-1}\}_{KS}$$

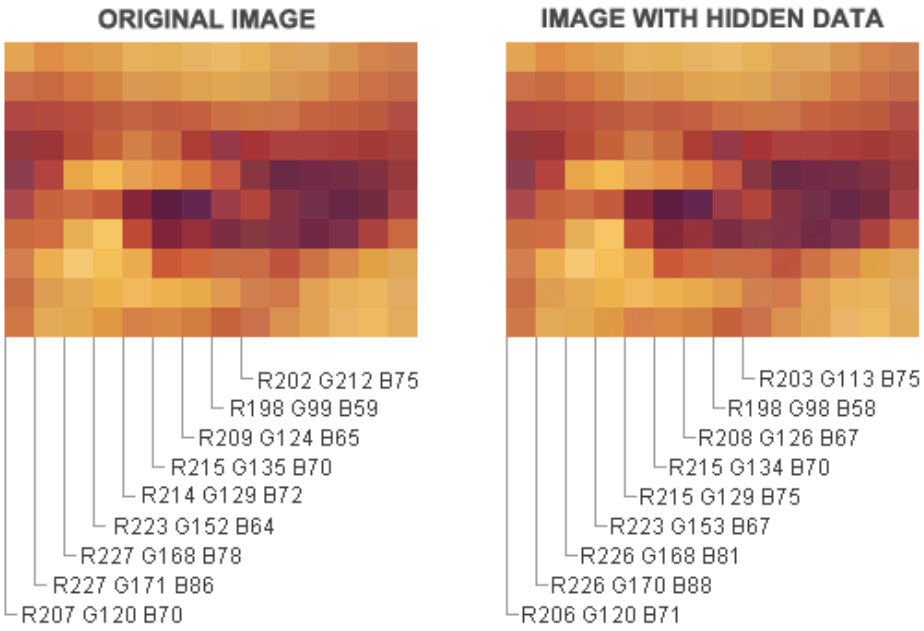
- Encrypting isn't always enough
- Encryption has to be resistant to rubber-hose cryptoanalysis



Related xkcd

Steganography

- Steganography – hiding data in data
- Hide message in the least significant bits of an image
- Steganographic file system
- TrueCrypt



Credit: easysector.com

Summary

- Some of the most challenging security engineering today have to do with the new online applications sweeping the world
- What goes wrong is just the same as we've seen elsewhere – the move to online applications was accompanied by a litany of bugs and security issues
- As more and more of our lives move online, the criticality and complexity of online applications grow