The Bleeding Edge

COMPUTER SECURITY SEMINAR

SPRING 2017

TOMER PELED

Outline

- Introduction
- Computer Games
- Web Apps
- Privacy and Anonymity
- Electronic Elections

Introduction

- The bleeding edge:
  the most advanced stage of a technology, usually experimental and risky
- The book is a little outdated – the bleeding edge of 2007 is old news today, however we will try to stick to the ideas and examples when relevant
- However, the ideas remain valid
  - Frauds are easier online
  - We depend on services and information that we did not verify

Computer Games

- Many games today are web-based
- There are many reasons to cheat on games
- Cheating in multiplayer games can take few shapes:
  - Breaking into games servers, decompiling executables to find bugs
  - Using flows in the game design – slow internet connection in shooting games
  - Using programming skills to get unfair advantage – scrapping online management games, using bots to play games while the user is away

Computer Games

- Unlike some other cases, the industry does its best to provide protection, as it harms their profits
- Detecting and exposing cheaters
  - Replays in shooting games show events from the other side point of view
  - Monitoring the network traffic/geo location
  - Monitoring online markets for illegal traders
  - Pattern mining of users behavior records.
- Preventing cheating actively
  - Encryption of network traffic
  - Bot traps

Computer Games – Bot Traps

- Bot is a program that automates tasks for the user
  - In real time 24/7 strategy games – can defend player's base
  - In management games – can collect and store data (and analyze it)
- Google's Captcha
  - In websites – type a word to prove you're not a bot – can be broken by some OCRs or just by cheap workforce from India
  - In mobile apps – just a simple checkbox as typing is not as natural
  - The new generation of Captcha – no implicit input by the user

Web/Mobile Applications

- As we said, many computer games are actually web/mobile apps
  - But they are also different
- Many of the people on the web are not aware of the dangers
  - Little kids, old people
  - Software engineers
- Many of the developers are not aware of the dangers
  - Heavily dependent turn-key solutions
  - Security is not on the priorities list
  - Search for ‘remove password’ commits in github

Web/Mobile Applications

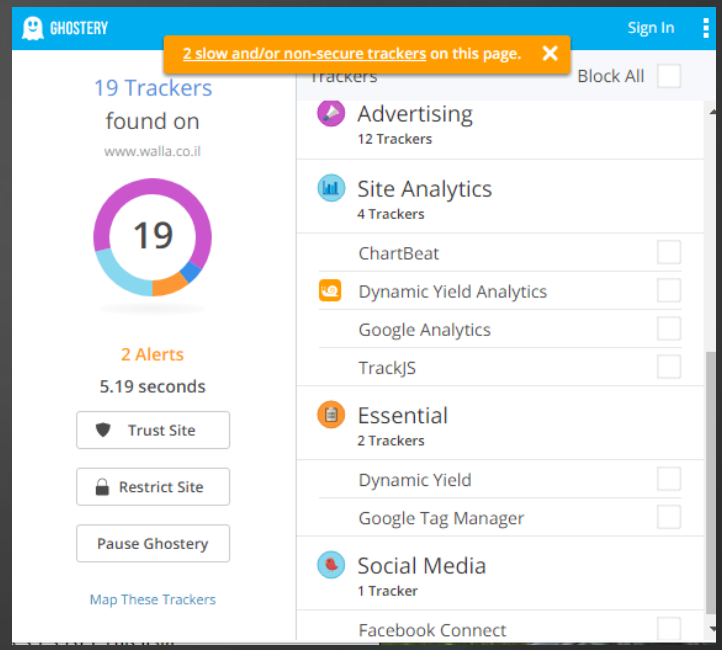
- Web development depends heavily on 3rd party libraries (usually open source)
  - Although those libs are open to public inspection, they are usually not designed with security in mind
  - They also have their own dependencies
  - The left-pad crisis – the guy who broke the internet
- HTTP Vs HTTPS
  - Today, a little more than half of the web browsing is done using HTTPS
  - Most of the big websites/services had moved to HTTPS as a default protocol in the last years, but still allow HTTP or unsecure SSL/TLS configurations

Privacy and Anonymity

- Privacy: when you want to do something without everyone knowing about it
  - Private discussions with friends/coworkers
  - Searching medical information online
  - LGBT communities and individuals in countries such as Russia, Iran
- Anonymity: when you want to do something that will be public, but do not want to expose yourself
  - Anti-government activists around the world
- Both terms are closely related and can affect each other

Threats on Privacy

- Our lives move online
  - We shop at Amazon and EBay, we spend money using PayPal, our social lives are on Facebook
  - All those companies and many more track us, many times without our consent and/or knowledge
- In some cases we benefit from it
- But in most cases we are just being stalked



Privacy – Facebook as an example

- Frequent changes in privacy default settings
- Sometimes even just ignore them – 'photos of..'
- Following users outside of Facebook itself
  - Login with Facebook account
  - Embedded code in other sites
- Facebook products, such as React are used in many websites/mobile apps
  - Facebook changing React's license – allowing them use IPs of anyone that use React

Privacy – Facebook as an example

- How far will Facebook go?
  - Conducting psychological experiments on users
  - Selling ads targeted to teenagers when they are psychologically vulnerable
  - Does Facebook listen to us?

Privacy and Anonymity Protection

- Proxies
  - Basically – routing the network through a 3rd party location so it will be harder to find the origin of the traffic
  - In reality – traffic is not encrypted, proxies may alter the traffic, and sometimes even send the package with information regarding its origins
  - Can be used to bypass geographic restriction
- VPN services
  - Somewhat similar to proxy but the traffic to the exit node is encrypted
  - Provides anonymity
  - Cons – logging policies differ between services, adds overhead

Privacy and Anonymity Protection

- Tor – The Onion Router
  - Package sent to Tor will be routed through several servers in the network before going out to the web again, each encrypting only what it needs to know (where to send it and where did it come from)
  - Servers are hosted by volunteers (and Governments)
  - Tor has weaknesses
    - Nodes can be hosted by eavesdroppers.
    - The exit node fully encrypts the data (the Tor encryption)
    - Tor will slow down the traffic
- Solutions can be combined – VPN + Tor

Privacy and Anonymity protection

- Bitcoin as a replacement to cash
  - India banning large bills
  - The Knesset discuss limitations on cash usage
- Tracking the trackers
  - Lightbeam/Ghostery – browser add-ons that track ‘hidden’ network requests while you browse the web to create a map sites/services you interact with without knowing
  - Allows you to inspect which of the websites your browse is untrustable/does not respect your privacy
  - https://www.ted.com/talks/gary_kovacs_tracking_the_trackers/transcript?language=en#t-245534

Electronic Elections

- What's wrong with regular elections?
  - Slow, cumbersome, expensive
- There are several mandatory requirements for elections
  - The voter must be a legitimate voter
  - The voter can't vote twice
  - The system must ensure that the vote was counted as the voter cast it
  - The voter can't prove to anyone else how she/he voted
- There are several different implementation for EE
  - The US model
  - The Estonian model

Electronic Elections - USA

- Based on special equipment – hardware and software
- Varies between different states and sometimes even different districts
- Electronic tracking
  - Voter fills the election form (manually or using a computer)
  - The form is scanned by a special EE equipment and can be kept for verification later
  - There are different variations in implementation
- Electronic voting
  - The voter choose the candidates using the equipment, no physical tracking
- There are some exceptions – old/sick people can vote by email

Electronic Election - USA

- There are several major issues
  - Until recently there was no security standard for EE equipment
  - Equipment is expensive and doesn't have a budget
  - Depending on the state, authentication is weak
  - Need to trust the EE equipment manufacturers, lack of transparency

Electronic Elections - Estonia

- Few relevant details
  - Estonia is internet based country – elections, taxes
  - You can have internet access everywhere
  - Highest rate of startups per capita in Europe
  - Citizens hold smart IDs
- Internet based elections
  - Every citizen can vote online using her/his smart ID
  - The number of internet voters grows steadily (~30% in 2015)

Electronic Election - Estonia

- Pros
  - Unlike the US model, cheaper to update the system
  - Easier to vote (and to manage all citizen-government interaction)
  - Source code is available on Github
- Cons
  - The internet is not safe, the elections are exposed to many attacks
    - Client side malware can change the vote
    - Server side malware can change the count
    - Voters can technically prove who they voted for
    - At 2014, a group of security researches who analyzed the system recommended the Estonian government to stop using it
  - The model doesn't necessarily fit other countries

Electronic Elections

- Other solutions can be found in between those 2 models
  - Software based EE that is not open on the internet
  - Cryptocurrency based elections (Offered in Victoria, Australia)
  - Partially electronic elections – even electronic authentication alone would dramatically improve Israeli elections

Questions?