DSci529:
Security and Privacy
In Informatics

Privacy Preserving Tech (continued)
Miscellaneous Topics
The Future of Security and Privacy
(for good or bad)
Review for Final Exam

Prof. Clifford Neuman

Lecture 14
23 April 2021
Online

Friday May 7th - Final Exam

The Final exam for DSci529 will be held Friday May 7th from 11AM to 1PM PDT.

- An alternate time will be provided for those with scheduling conflicts (e.g. because of their time-zone)
- At 11AM (or an alternate time) two files will e-mailed to all students:
  - A word document with the exam
  - A text document with the exam
- You will complete the exam in word or any other text editor of your choice and upload exam to D2L Dropbox by 1:15 PM (15 minutes added for logistics, etc)
- The exam will include a self certification that you neither gave nor received any assistance during the exam.

Discussion and Review for the Exam later in Lecture

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:30 Privacy Preserving Technologies (continued)
12:30 – 13:30 Student Presentations – Miscellaneous
- Yo-Shuan Liu – Usable Security
- Philana Williams – Security for Web App Development
- Haonan Xu – Privacy issues in Cloud Computing
- Pratishtha Singh – Card privacy Concerns in India
- Yilin Zhang - Blockchain and Data Security

13:30 – 13:40 Break
13:40 – 14:55 Class Discussion – Mass Surveillance
14:55 – 14:15 China's Social Credit Score
14:15 – 14:50 Review for Final Exam
14:50 – 13:20 Current Event Discussions

Privacy Preserving Technologies

Technologies that can be employed by users to improve their privacy and security.

And the negative implications of these technologies.

Storage Encryption

- File Sharing (not necessarily encrypted)
- TrueCrypt
- PGP

- THESE WERE COVERED AT THE END OF THE PREVIOUS LECTURE

Some Readings on The Dark Web

- Readings:
  - Time Magazine **The Secret Web: Where Drugs, Porn and Murder Live Online November 11, 2013.**
  - It's About To Get Even Easier to Hide on the Dark Web, Wired 1/28/2017.
  - https://www.vice.com/en_us/article/ezv85m/problem-the-government-still-doesnt-understand-the-dark-web
  - **US government funds controversial Dark Web effort**

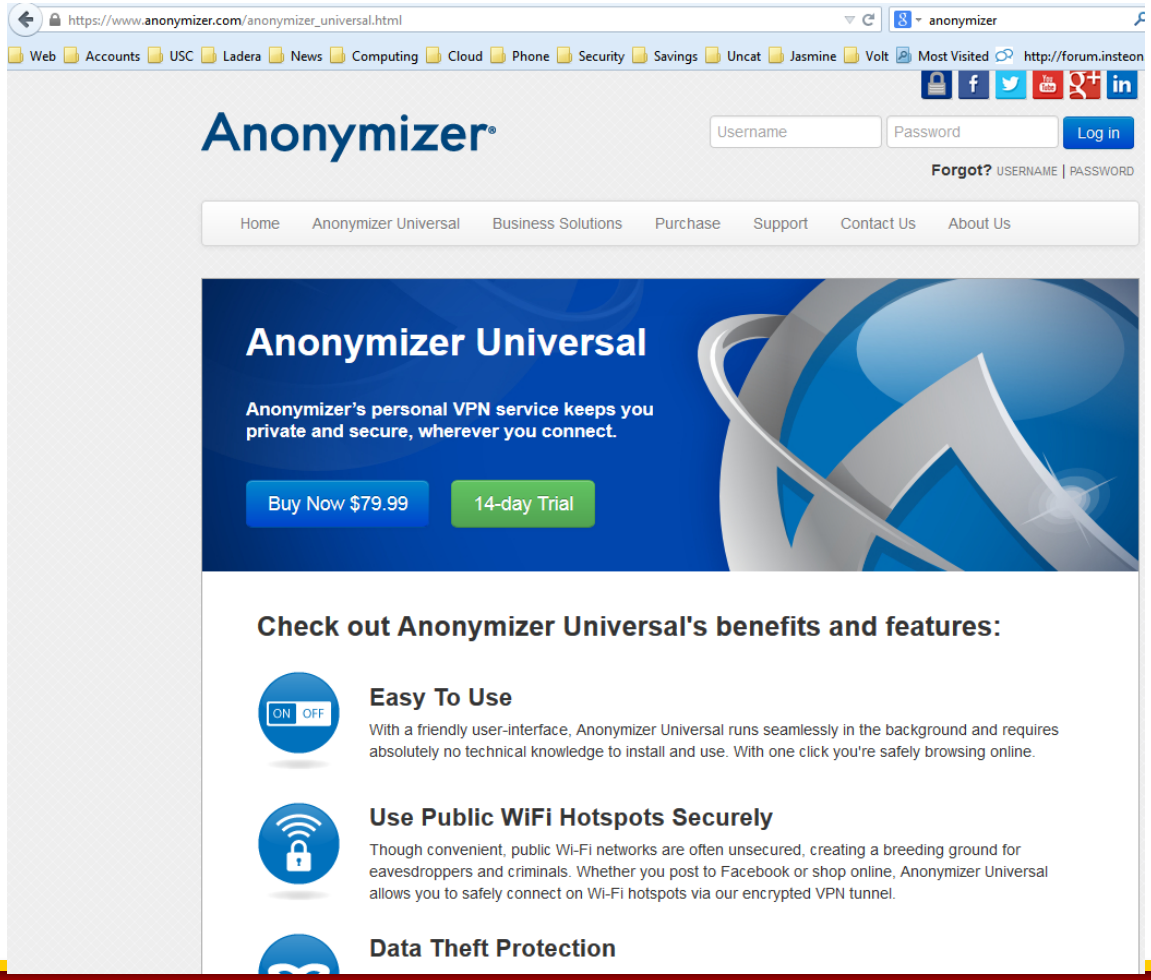
Anonymization

- For internet communication (email, web traffic) even if contents are protected, traffic analysis is still possible, providing information about what sites one visits, or information to the site about your identity.

- Tools are available that will hide your addresses
  - Proxies
  - Networks of Proxies – Onion Routing and TOR

Anonymizer and similar services

- Some are VPN based and hide IP addressed.
- Some of proxy based, where you configure your web browser.
- Need the proxy to hide cookies and header information provided by browser.
- You trust the provider to hide your details.
- Systems like TOR do better because you don’t depend on a single provider.



TOR

- Originally developed by US Navy to protect Internet communications
- The problem:
  - Internet packets have two parts – header and payload
  - Even if payload is encrypted, header is not
  - Header lists originator and destination nodes – all nodes along the way can read this information
- Why might this be a problem:
  - Law enforcement or criminals may not want it known they are visiting a site
  - General privacy protection.

TOR


WHISTLEBLOWER
AID
LEGAL ADVICE
FOR PATRIOTS.
AFFORDABLE AND
CONFIDENTIAL.
Learn more at:
whistleblowersaid.org
Anonymous access using Tor Browser:
wbaidlaw6quwv7h3.onion

TOR

- Continued development and improvement with US funding (Dept of State)
- SAFER project:
  - Develop improvements or similar technologies that are less vulnerable to persistent attempts to track users, e.g. dissidents, etc.

TOR

From Engadget, 7/28/2014

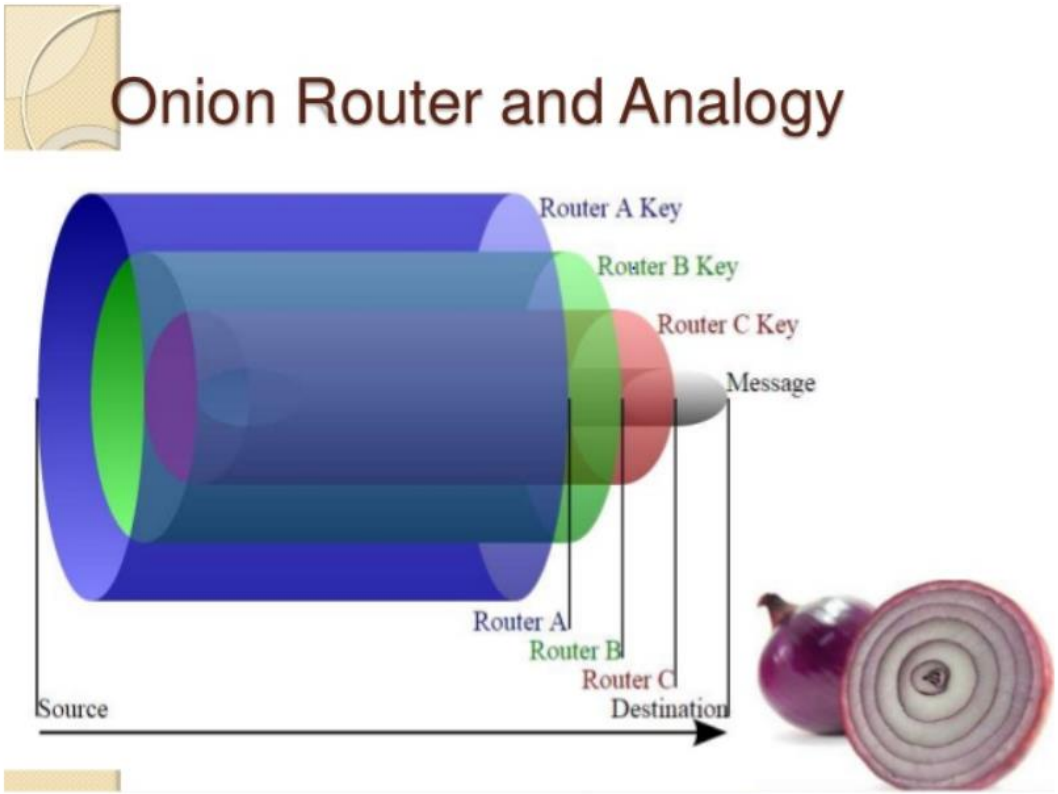
Russia offers a $110,000 bounty if you can crack Tor

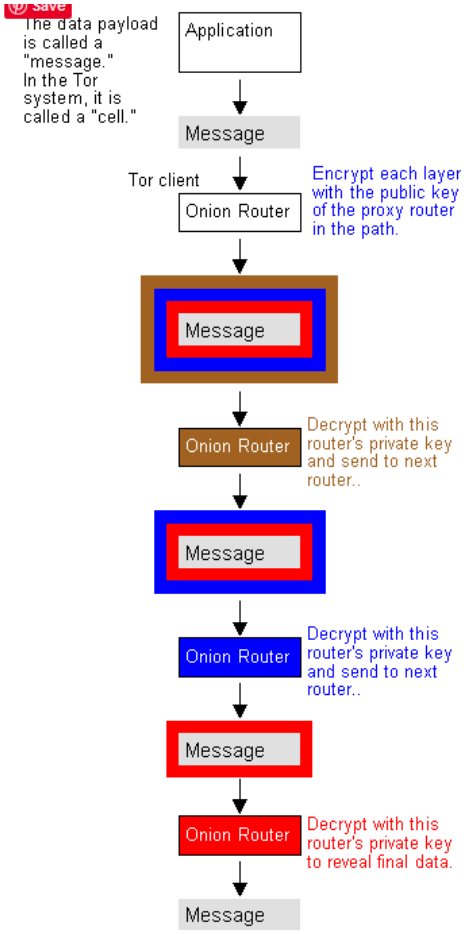
Countries that have less-than-stellar records when it comes to dissenting voices must really, really hate Tor. Coincidentally, Russia's Interior Ministry has put out a bounty of around $110,000 to groups who can crack the US Navy-designed privacy network. After the country's vicious crackdown on dissenting voices back in 2012, protestors who hadn't escaped or been jailed began using anonymous internet communication as their first line of defense against the Kremlin. If you're considering taking part in the challenge (and earning yourself a tidy stack of cash to quell your conscious), be warned -- the bounty is only open to organizations that already have security clearance to work for the Russian government.

TOR - Fundamentals

- Origin node accesses list of TOR nodes and creates the packet:
- Starts by creating a packet consisting of payload and header – header contains desired destination node and final TOR node in zigzag route
- Now treats the above packet as a payload and creates a header with origin and destination consisting of two TOR nodes
- This is repeated until final packet contains a header with original source node and first TOR node identified
- …**Hence the term "Onion Routing"**

TOR – Fundamentals





Source cybersolutons.ga and yourdictionary.com

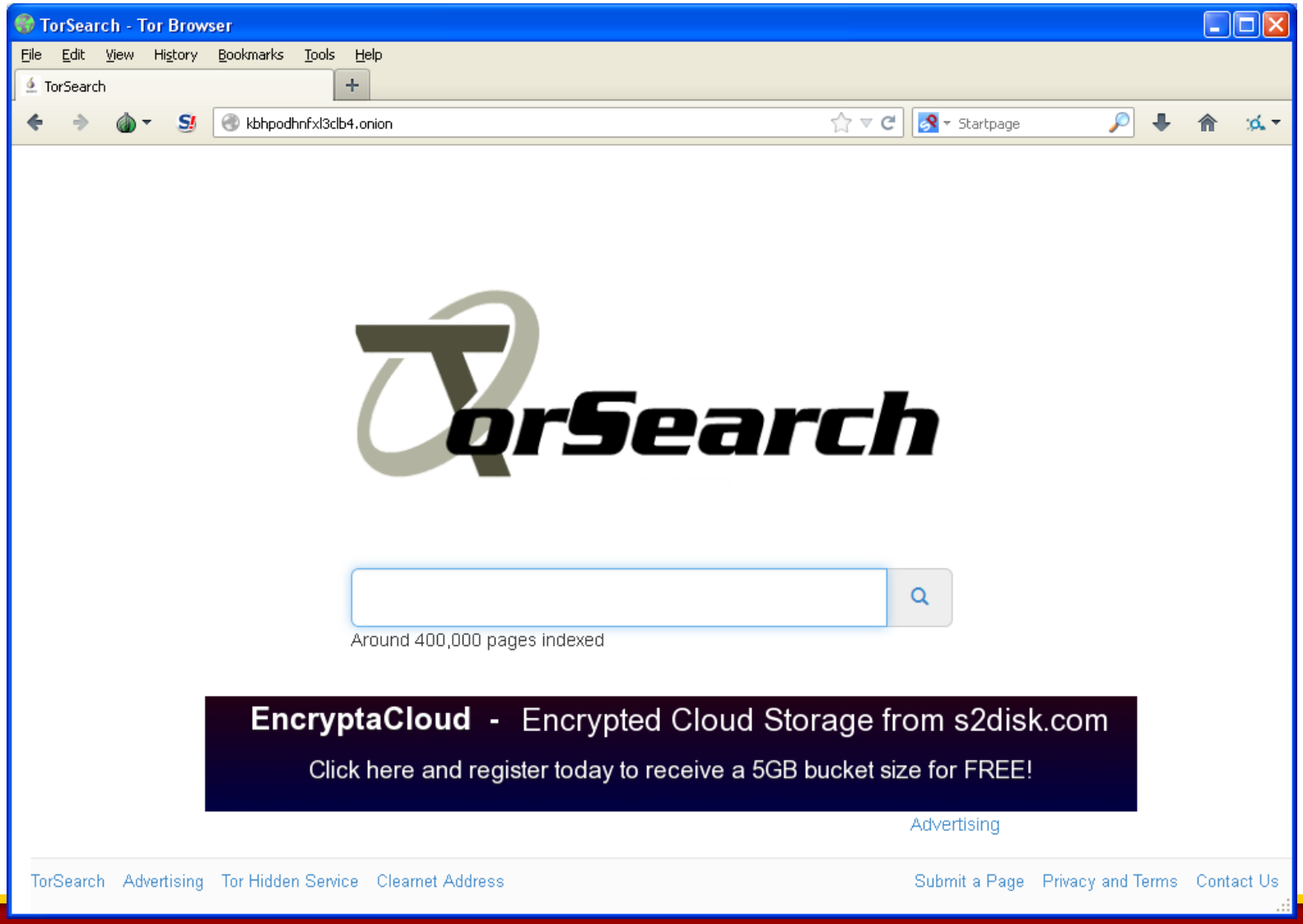
TOR - Fundamentals

- List of TOR nodes periodically changes
- Zigzag route is periodically changed

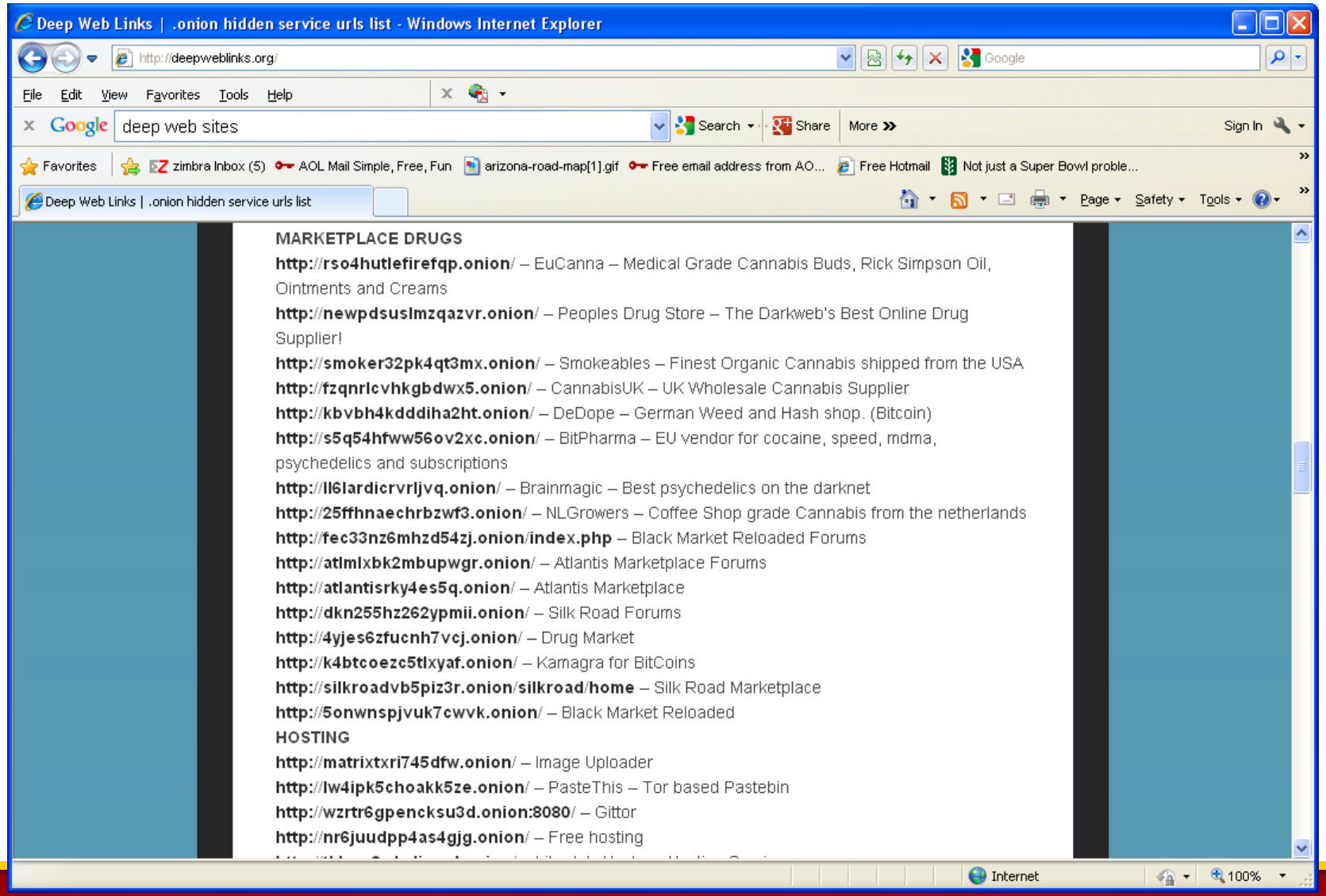
- Not totally fool proof:
  - If non-TOR browser opened within TOR browser, security measures are void – basically going back to “direct routing”
  - Someone monitoring source and destination node may note synchronization of packets being sent/received.
    - …**to avoid: increase TOR traffic**


About Tor - Tor Browser
File Edit View History Bookmarks Tools Help
About Tor
about:tor
Startpage
Tor Br
3.6.3-Wi
Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Startpage.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
Run a Tor Relay Node »
Volunteer Your Services »
Make a Donation »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

TorSearch - http://kbhpodhnfxl3clb4.onion/

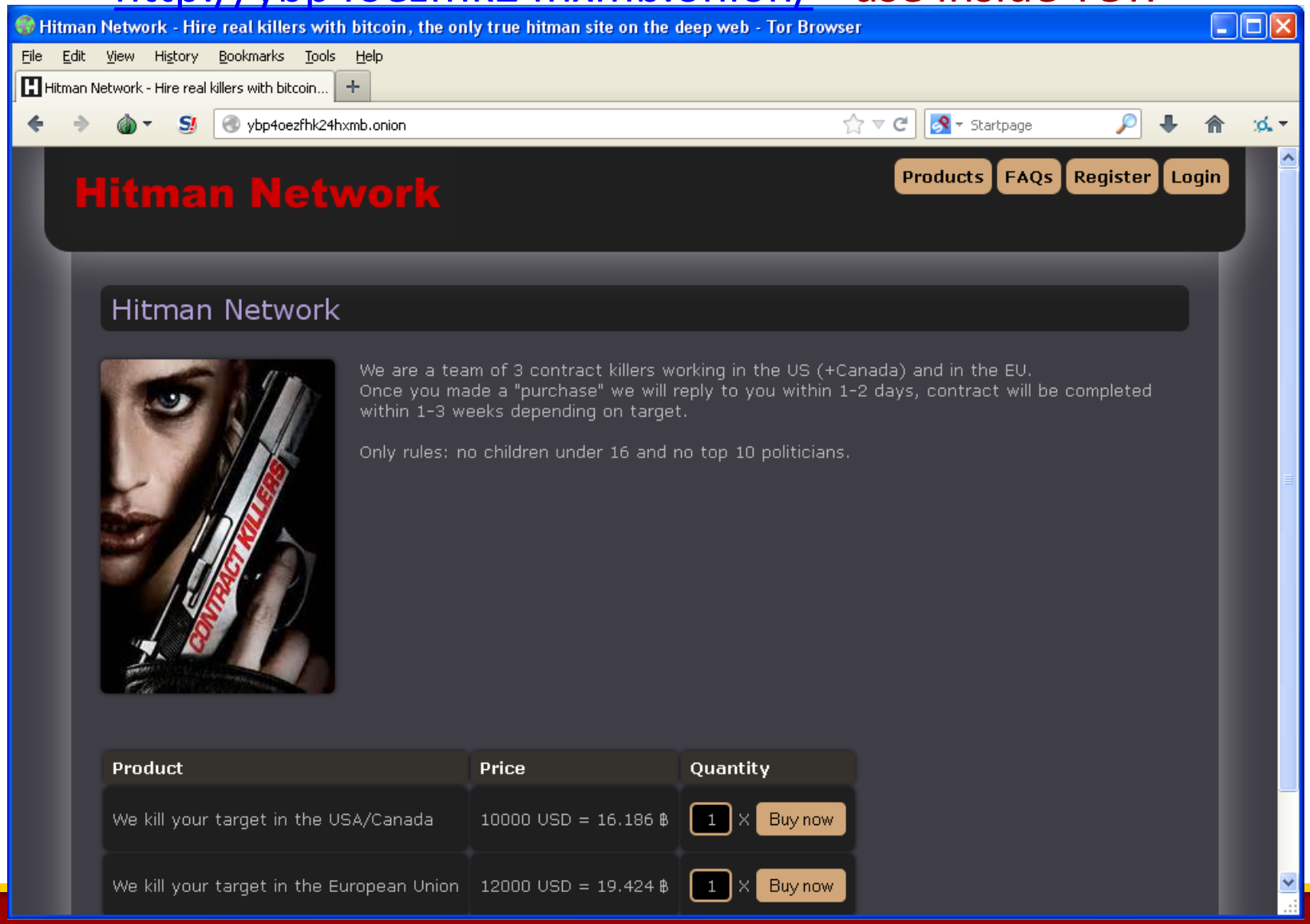


http://deepweblinks.org/



http://2ogmrlfzdthnwkez.onion/ - use inside TOR

http://ybp4oezfhk24hxmb.onion/ - use inside TOR



http://xfnwyig7olypdq5r.onion/ - use inside TOR

Discussion

- Readings:
  - Society deserves privacy, but at what cost.
  - Who defines “good use”
  - Dark v. Deep Web
  - How to control the dark web (technically)

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:30 Privacy Preserving Technologies (continued)
12:30 – 13:30 Student Presentations – Miscellaneous
- Yo-Shuan Liu – Usable Security
- Philana Williams – Security for Web App Development
- Haonan Xu – Privacy issues in Cloud Computing
- Pratishtha Singh – Card privacy Concerns in India
- Yilin Zhang - Blockchain and Data Security

13:30 – 13:40 Break
13:40 – 14:55 Class Discussion – Mass Surveillance
14:55 – 14:15 China's Social Credit Score
14:15 – 14:50 Review for Final Exam
14:50 – 13:20 Current Event Discussions

SECURITY & UX DESIGN

Usable Security

DSCI 529

Yo Shuan Liu

What is User Experience (UX)

- User experience (UX) design is the process of creating products that provide meaningful and relevant experiences to users.

- This involves the design of the entire process of acquiring and integrating the product, including aspects of branding, design, usability and function.

Why is Usable Security Important?

"Security must be usable by persons ranging from nontechnical users to experts and system administrators. Furthermore, systems must be usable while maintaining security. In the absence of usable security, there is ultimately no effective security."

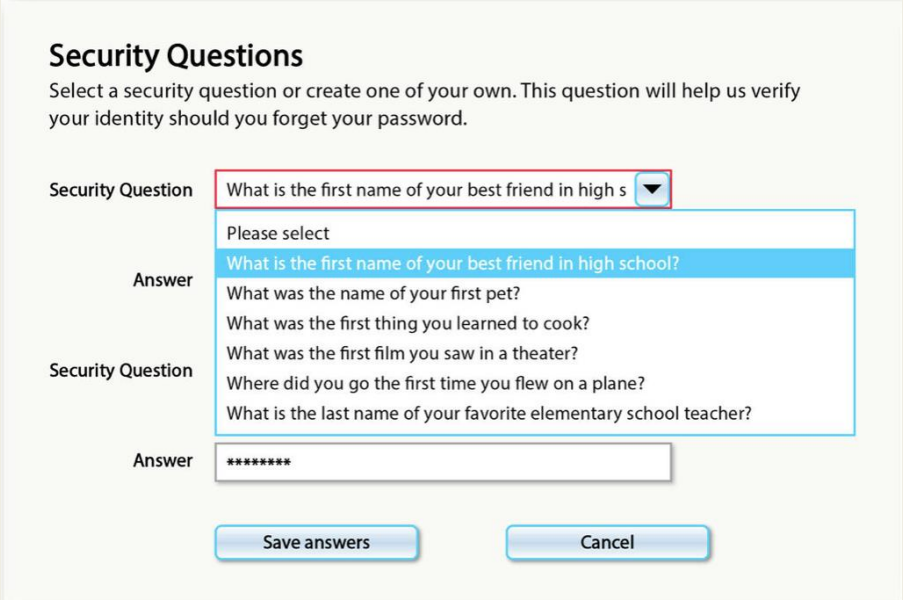
- US Department of Homeland Security Nov 2009

“People will find ways to bypass your unusable security”

“Some security process’ cost are more than it’s worth”

A bike attempting to look secure.

“Obscurity only increases security until it doesn’t”



Picture from: The Wall Street Journal

How to Find an Appropriate Balance?

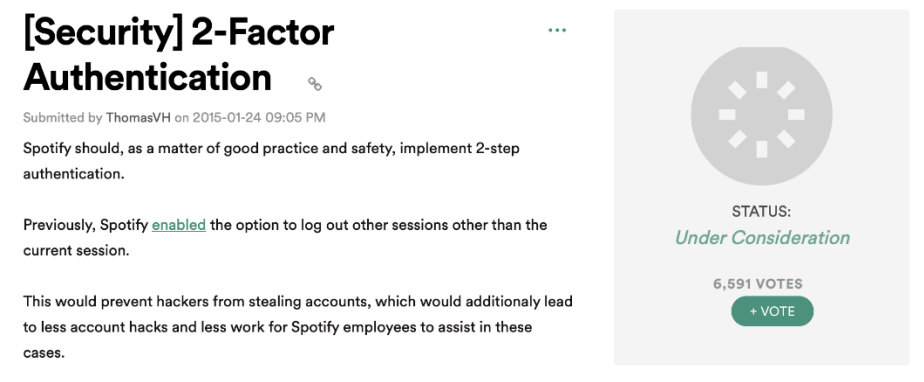
Some important things to consider and questions to ask before designing the security flow..

Security Regulations of the Product

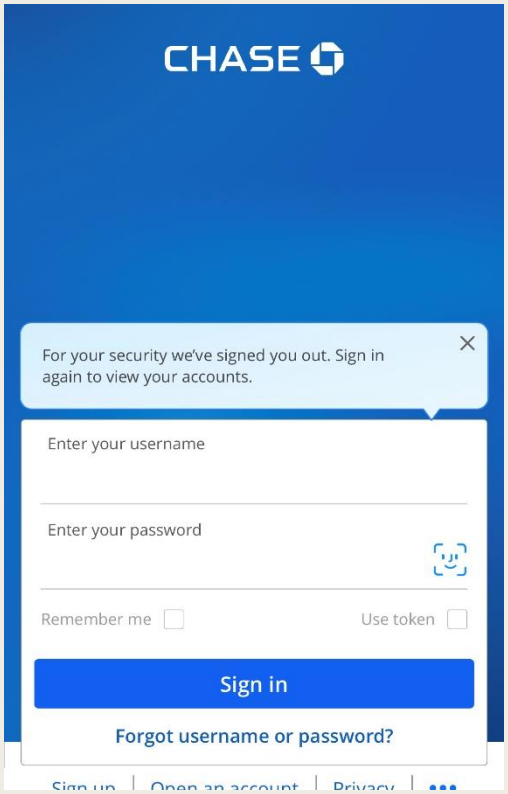
- Designers ought to be aware of the various security regulations that apply to the digital products they work on.
- E.g. HIPPA for the healthcare industry, and PCI DSS for banking and financial services.

Level of Security

- How much security do you actually need?
- Some types of product will require much heavier security.



A open feature request for MFA on Spotify community on 2015.



Questions to Ask

- 1. How to authenticate?
- 2. When to initiate authentication?
- 3. Who needs to be authenticated?

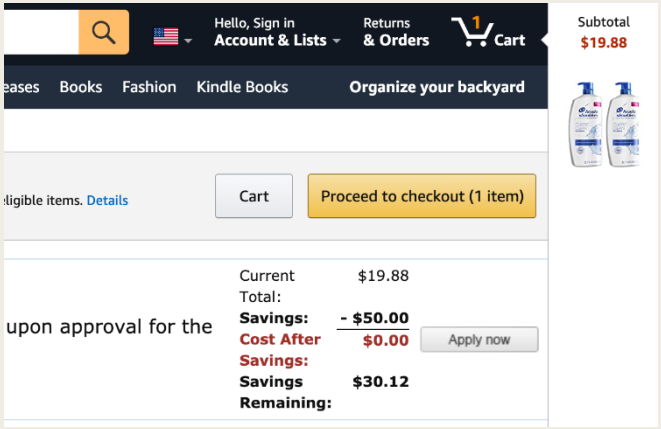
1. How to Authenticate?

- Common types of Authentication: Password-based authentication, Multi-factor authentication, Biometric authentication, …



2. When to Initiate Authentication?

- Each time when a user logs in
- When a new device is detected



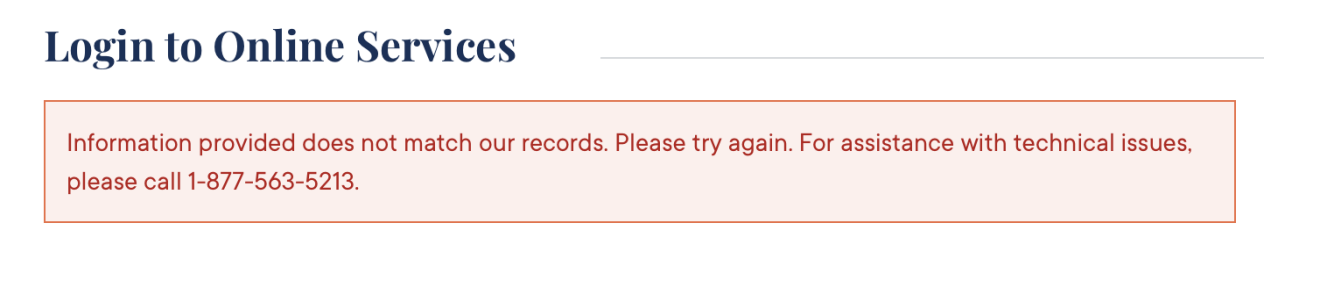
A great example of delaying authentication

3. Who Needs to be Authenticated?

- Mandatory
- Opt-in or opt-out
- Risk-based authentication (Adaptive authentication)

When fails, fail gracefully

- Clear feedback in error scenario



DMV Login: An example of not having a clear error message.

- A good security system should have plan B and C
- Don’t make users feel like a criminal

Other Heuristics to Follow

- Consistency and standards: Don’t reinvent the wheel. Follow patterns that exist across platforms.

- Visibility of system status: It’s good to have a bar indicating which authentication step the user is in and how many more steps left.

- If you want user to perform an action (e.g. go to email and click the link), make the call to action (CTA) text clear and large.

Conclusion

- More security doesn't always lead to more secure users
- Be realistic and reasonable
- Get stakeholders – security experts, engineers and designers, involved in UX security early
- Embrace the fact that you will always have some level of insecurity in your design
- Good UX leads to great security

Reference

- https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap_0.pdf
- https://medium.com/nyc-design/a-tale-of-three-doors-security-ux-design-8746f7663dae
- https://uxdesign.cc/how-good-ux-leads-to-great-security-293327c83a90
- https://uxdesign.cc/feature-teardown-my-epic-fail-in-building-a-multi-factor-authentication-694e403324f3
- https://www.toptal.com/designers/product-design/ux-security

Security for Web Application Development

PHILANA WILLIAMS

DSCI 529

Agenda

1. Key Definitions
2. Web Application Mechanics
3. Motivations and Opportunities for Exploitation
4. Web Application Attacks
5. Web Application Security Measures

Key Definitions

Web Application – Software that allows users to send and retrieve data from a web server, using their preferred browser.

Web page – A document that can be displayed on a web browser

Website – Group of web pages connected in various ways (ie my.usc.edu and classes.usc.edu)

Web server – A computer used to host a website on the Internet

Key Definitions

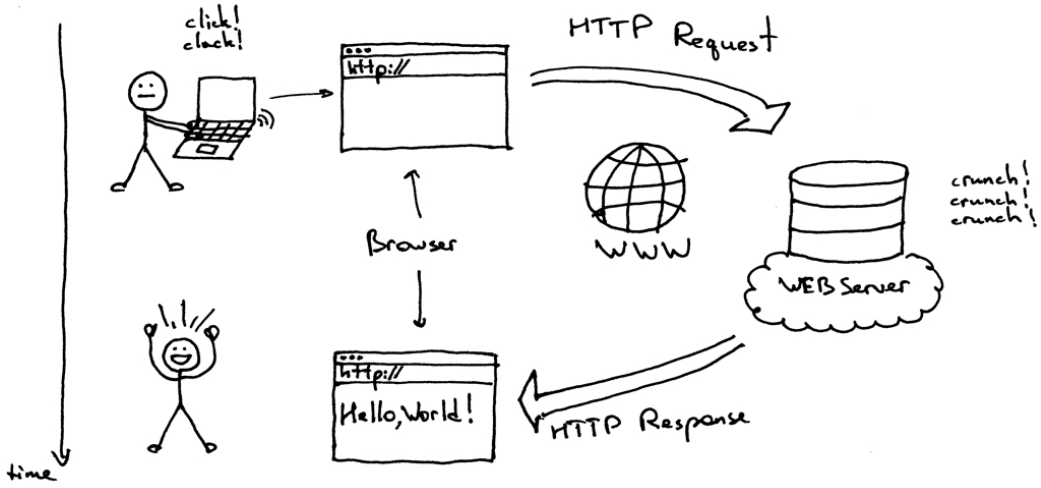
HTML (Hyper Text Markup Language) – Human readable file format that describes the structure of elements that exist within a webpage.

CSS (Cascading Stylesheet) – Human readable file format that controls the formatting and styling of HTML elements

JavaScript – Client-side scripting language embedded into HTML document, used to execute tasks within the browser, as user interacts with a webpage

Web Application Mechanics

1. User sends HTTP request to a web server by enter a URL into their preferred browser
2. Web server receives the request, executes tasks, performs databases operations, depending on the data included in the request and the programming logic of the web application
3. A response is generated by the web application, and this response gets sent from the web server back to the user's browser.
4. The browser displays data received in the HTTP response



Motivations and Opportunities for Exploitation

1. Websites and must be available 24/7, in order provide required services

2. Web applications must be available to the public internet, so they can not be hidden behind port-level firewalls.

3. Web applications that collect and store user data have direct access to databases that may contain sensitive (and very lucrative) user information.

4. Most web applications are custom-made and subject to less testing than commercial software made for a specific operating system

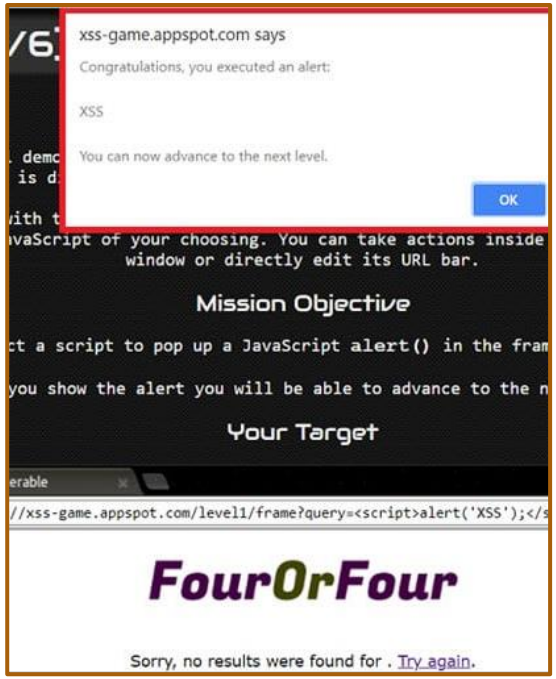
Web Application Attacks – Cross-Site Scripting

Attackers embed malicious code into the HTML file used to display the webpage in browser

Websites are vulnerable to this type of attack when they use user input or URL parameters to generate outputs to display to the browser.

When user inputs are displayed to the browser, this is with the help of a client-side scripting language, that dynamically creates and/or modified existing elements within the webpage's HTML

Attacks possible using scripting languages such as JavaScript, VBScript, Flash, ActiveX, and CSS

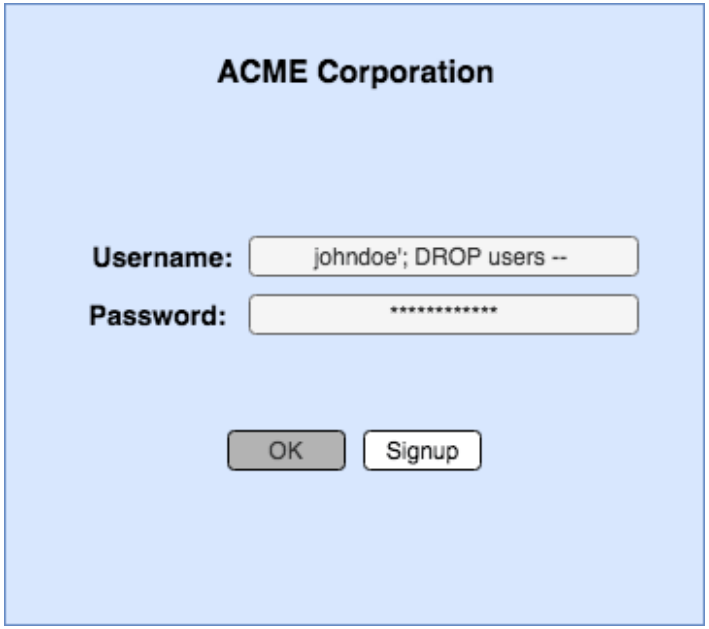


Web Application Attacks – SQL Injection

Attackers target server-side databases directly by embedding malicious SQL queries into user input fields or URL parameters

SQL injections made up **65%** of web-based attacks from 2017 to 2019

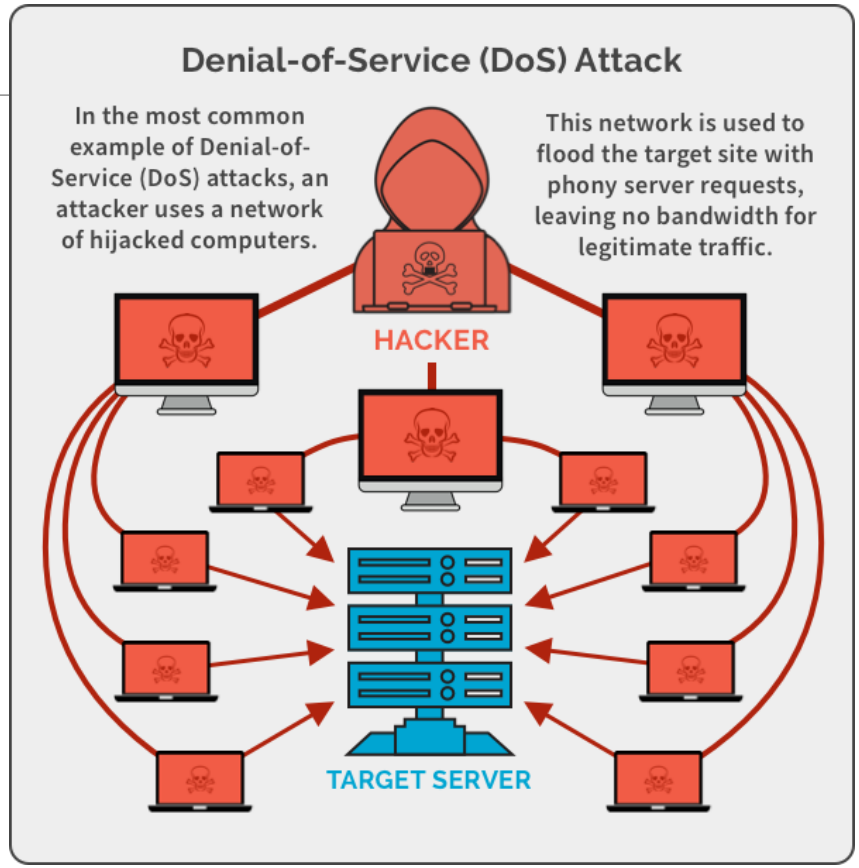
Common SQL injection attack include adding “OR 1 = 1” or “OR ‘=‘“ to force conditional “WHERE” clauses to always be TRUE



Web Application Attacks – Denial of Service

Attacker overwhelms web application with too many requests, making it impossible to serve legitimate users of the website

This attack can be carried out using automated means, such as bots that spam requests to a site



Web Application Attacks – Directory Transversal

The root directory of a web server's file system defines the specific directory level that users are confined to.

This restriction is an important precaution against unwanted modification of critical system files, by users of the system.

Attackers use Directory Transversal attacks to access restricted directories and execute commands outside of the web server's root directory

```
GET http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini HTTP/1.1
Host: test.webarticles.com
```

Web Application Security Measures

1. Escaping user input
   - Prevents malicious interpretation of user input by censoring characters that may be interpreted as HTML elements or script tags (mainly “<“ or “>”)
2. Input validation
   - Checks if user input is a subset of a ‘trusted’ group, before using the data in client-side scripts or database queries (ie: a text field that only allows alphabetical characters)
3. Input sanitization
   - Modifications made to user input to make sure that it is valid, before using the data in client-side scripts or database queries (ie: stripping user input of white space, and encapsulating input in double quotes)

Web Application Security Measures

4. SQL binding parameters
   - Alternative method of passing data to database rather than writing values from user input directly into the SQL statement. Instead, a SQL query is prepared, using placeholder values. The actual values are then passed to the prepared query in a manner that enforces data types and protects against malicious SQL injection.

5. Intrusion Prevention / Intrusion Detection System
   - Software such as a web application firewall, that uses rules and intelligence about breach tactics (ie anomalous user behavior or network traffic) to restrict access to applications.

References

1. What is the difference between webpage, website, web server, and search engine? - Learn web development | MDN (mozilla.org)
2. Web Server Definition (techterms.com)
3. SQL Injection Attacks on the Rise, As Gaming Industry Under Attack from Credential Stuffing (techmonitor.ai)
4. What is Cross-site Scripting and How Can You Fix it? (acunetix.com)
5. Introduction to HTML (w3schools.com)
6. State of the Internet / Security | Web Attacks and Gaming Abuse (Volume 5, Issue 3) | Akamai
7. SQL Injection (w3schools.com)
8. Denial of Service (DoS) guidance - NCSC.GOV.UK
9. File Inclusion Vulnerabilities - Metasploit Unleashed (offensive-security.com)
10. Understanding SQL Injection and Prevention using Parameter Binding in PHP - DEV Community
11. Web Applications Attacks - Common Types of Web Based Attacks (trustnetinc.com)
12. WAF Meaning & Definition | What is Web Application Firewall? (esecurityplanet.com)

Questions?

Privacy in Cloud Computing

DSCI 529 Haonan Xu

What is Cloud Computing?

- Definition
  - "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

- Why Cloud Computing?
  - Optimized resource management
    - Resources refer to computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure.
  - **Not only ‘computing’ but also data storage**

How do we access Cloud Computing services?

- 3 Common commonly used service models:
  - SaaS (Software as a Service)
    - Cloud service providers provides software applications, and users can use it through a client interface such as a web browser
    - E.g. Web-based email such as Gmail; CRM from Salesforce
  - PaaS (Platform as a Service)
    - Cloud providers provides tools that enable developers to deploy applications
    - E.g. Google App Engine; Salesforce's Force.com
  - IaaS (Infrastructure as a Service)
    - The cloud service provider facilitates services to the users with virtual machines and storage to improve their business capabilities.
    - E.g. Amazon EC2 Web Service

Internet and Privacy

- Properties of the Internet that threatens privacy:

  - Openness
  - Virtuality
  - Interactivity
  - Anonymity

Privacy Issues in Cloud Environment

- The storage and security of data
  - Entirely the responsibility of the cloud computing provider.
- Distributed Architecture
  - Data segments are separately distributed over the cloud
- Data Transferring
  - Outside attack during transmissions

How to deal with the problems?

- Improve legislation and related legal systems
  - From a legal perspective, the right to privacy in the cloud computing environment belongs to the right to internet data privacy.
- Improve Privacy Enhancing Technologies (PETs)
  - Reduce the risk of contravening privacy principles and legislation.
  - Minimize the amount of data held about individuals.
  - Allow individuals to retain control of information about themselves at all times.
- Set up regulatory agencies
  - To achieve effective supervision of cloud computing services, a trusted third-party regulatory agency (possibly) led by the government can be established.

One PETs Example

- Amazon Web Service (AWS): Zelkova and Tiros
  - To deal with misconfiguration errors
  - Zelkova uses automated reasoning to analyze policies and the future consequences of those policies.
  - Tiros maps the connections among your networks.
- Another PETs example: IBM's Proventia Multi-Function Security (MFS)
  - It contains functionalities like intrusion prevention, shield vulnerabilities at the network level, ICSA-certified firewall, anti-virus and anti-spyware, web filter with more than 70 million catalogued websites, and etc.

References

https://journals.sagepub.com/doi/full/10.1155/2014/190903

https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf

https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing

https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-privacy-in-the-cloud-pov.PDF

https://www.acardia.co.uk/ibm/ibm-software/ibm-tivoli-experts/proventia-network-multi-function-security.html

https://www.csoonline.com/article/3298166/what-are-amazon-zelkova-and-tiros-aws-looks-to-reduce-s3-configuration-errors.html

Thank you!

PRIVACY CONCERNS WITH AADHAAR

- Pratishtha Singh

WHAT IS AADHAAR?

- Aadhaar is a 12-digit unique identification number issued by Unique Identification Authority of India (UIDAI)
- Any resident of India can voluntarily enroll to obtain Aadhaar number.
- Person willing to enroll has to provide minimal demographic and biometric information during the enrolment process.
- Aadhaar is the world's largest biometric ID system

PII COLLECTED BY AADHAAR

Demographic information	Name, Date of Birth (verified) or Age (declared), Gender, Address, Mobile Number (optional) and Email ID (optional), in case of Introducer-based enrolment- Introducer name and Introducer's Aadhaar number, in case of Head of Family based enrolmen- Name of Head of Family, Relationship and Head of Family's Aadhaar number; in case of enrolment of child- Enrolment ID or Aadhaar number of any one parent, Proof of Relationship (PoR) document
Biometric information	Ten Fingerprints, Two Iris Scans, and Facial Photograph

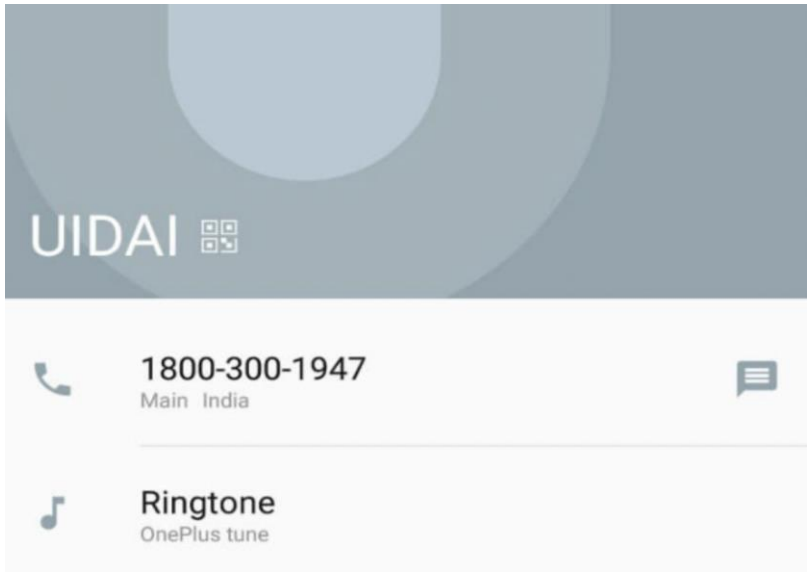
USES OF AADHAAR

- It can be used as a primary identifier to roll out several Government welfare schemes for effective service delivery.
- Resident can use the Aadhaar number to authenticate and establish their identity multiple times using electronic means or through offline verification.

PRIVACY CONCERNS

- **Identity theft**: Possible leakage of biometric and demographic data, either from the central Aadhaar repository or from a point-of-sale or an enrollment device.
- **Identification without consent** using Aadhaar data: There could be unauthorized use of biometrics to identify people illegally. The demographic data can be used to identify people without their consent and beyond legal provisions.
- **Correlation of identities across domains**: It may become possible to track an individual's activities across multiple domains of service using their global Aadhaar IDs.
- **Illegal tracking of individuals**: Individuals can be tracked or put under surveillance without proper authorization or legal sanction using the authentication and identification records. Such records may reveal information on location, time, and context of authentication and the services availed.

MYSTERIOUS PRIVACY BREACH



- This breach occurred in 2018. The helpline number of UIDAI was automatically added in the contact list of all Android users in India.
- UIDAI tried to distance itself from the helpline number controversy.
- Google took the blame, they called it an "inadvertent coding mistake".

OTHER SECURITY BREACHES

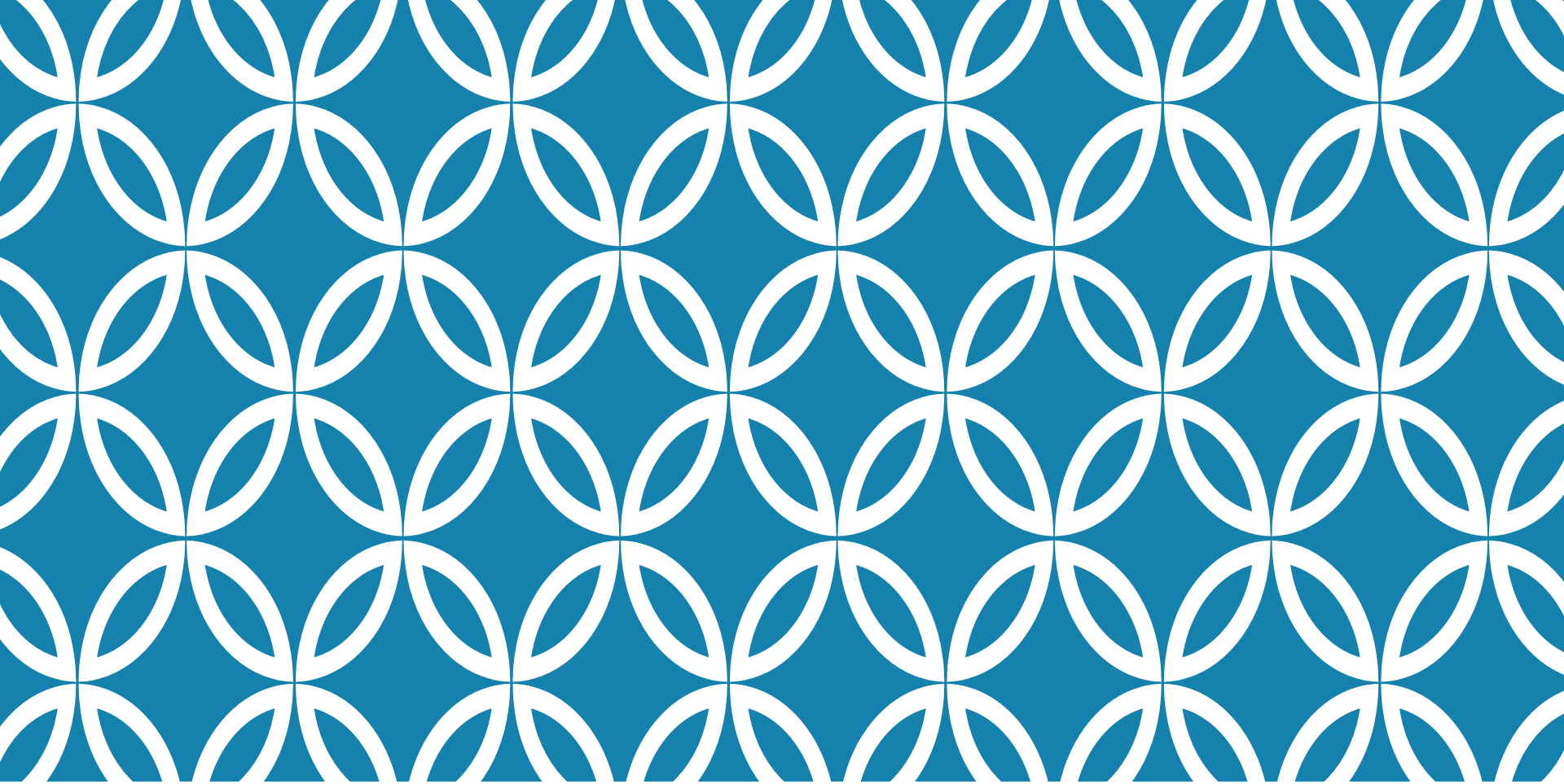
- French security researcher pointed flaws in the mAadhaar app by bypassing the password protection.
- RTI query pushed UIDAI to reveal that about multiple government websites made the Aadhaar details of people with Aadhaar, public on the internet.
- There have been a number of leaks of demographic data through third parties.

FUTURE OF AADHAAR

- Aadhaar number holders can secure their biometric authentication by locking their biometrics and Adhaar number.
- By Locking Aadhaar Number, resident will not be able to perform any Authentication using Aadhaar number. However, they can perform Authentication using Virtual ID.
- Not providing Aadhaar information to agencies that don't need it or cannot force to submit it.
- Adding a multiple factor authentication if someone tries to access information through QR code.

REFERENCES

- https://uidai.gov.in
- https://www.moneylife.in/article/aadhaar-is-a-mass-surveillance-tool-and-there-should-be-criminal-penalty-for-its-misuse-says-edward-snowden/55088.html
- https://cacm.acm.org/magazines/2019/11/240384-privacy-concerns-with-aadhaar/fulltext
- https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html



SECURITY AND PRIVACY ISSUES ON BLOCKCHAIN AND ITS APPLICATIONS

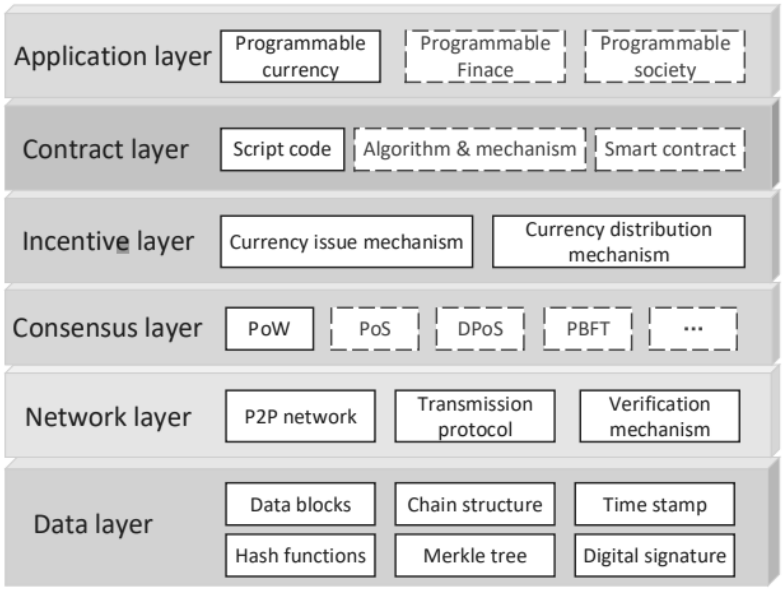
DSCI529 Security and Privacy in Informatics
Name: Yilin Zhang
USCID: 7800061647

OUTLINE

- What is Blockchain technology?
- How does Blockchain technology secure our data?
- How secure is Blockchain really?
- What are the solutions addressing security and privacy problems?
- Where is Blockchain used?

INTRODUCTION

- Decentralized, Shared, Immutable, Anonymity Public digital ledger
- Six Layers:
  - Data
  - Network
  - Consensus
  - Incentive
  - Contract
  - Application



SECURITY AND PRIVACY ON BLOCKCHAIN

- Integrity: encryption, immutability, data traceability on the chain
- Availability: decentralized architecture, consensus mechanism
- Anonymity of User's identity: pseudo-identity, multiple key pairs (addresses)
- Tamper-Resistance: hash function, digital sign, verification mechanism
- Resistance to DDoS Attacks: decentralized architecture, consensus mechanism

SECURE OR NOT?

- Confidentiality concerns
  - publicly available
  - lack of unlinkability
  - sequence and content of events stored on the Blockchain often reveal too much
  - forensically analyzed on cryptocurrency wallet software
  - identities exposed by the exchange
- Security shifted to the end user
  - no checks against fraud, mistakes, or loss
  - cryptographic cracking

SECURE OR NOT?

- 51% Attack

2020.07: over 270,000 bitcoin and cryptocurrency users' personal information published online by stolen from the popular France-based bitcoin wallet – Ledger.

- Program Bugs

It's not simple to fix a bug. The only way is to go back to the point before the attack, create a fork to a new blockchain, and have everyone on the network agree to use that one instead.

SOLUTIONS

- Membership service provider: user authentication, access control
- Privacy using channels: provide privacy between different ledgers
- Privacy using private data collection: ensure certain data confidentiality
- Smart contract confidentiality: authorized identity, endorsement policies
- Homomorphic Encryption (HE): achieve privacy-preserving computation
- Identity mixer: minimum disclosure, revocation

…

APPLICATION, NOT ONLY BITCOIN

- Healthcare
- Real estate
- Government
- Intellectual Property (music, book, etc.)
- Gaming
- Fintech, Cryptocurrency
- IOT, Could, Cybersecurity, Hardware, Software…

13 PROMINENT BLOCKCHAIN APPLICATIONS TO KNOW

- Secure sharing of medical data
- NFT marketplaces
- Music royalties tracking
- Cross-border payments
- Real-time IoT operating systems
- Personal identity security
- Anti-money laundering tracking system
- Supply chain and logistics monitoring
- Voting mechanism
- Advertising insights
- Original content creation
- Cryptocurrency exchange
- Real estate processing platform

HEALTHCARE

- Securely transfer sensitive medical information
- Manage patients' Electronic Healthcare Records (EHRs)
- Challenges:
  - different records may be accessible to different health professionals
  - needs to have adequate privacy: anonymous
  - right to be forgotten in GDPR

NFT(NON-FUNGIBLE TOKENS)

- Unique digital works of art and other collectibles that are trade on the blockchain
- Intellectual Property identifier
- Smart contract + NFT: how NFT can be used
- Challenges:

  - need marketplace: confidentiality concern

  - hack and steal purchased NFT: fishing, social engineer, malicious code…

  - authenticate false input: Art turned into NFT without the artist's knowledge

IOT

- Safe and auditable exchange of data
- Secure the IoT system
- Operating in an automated and decentralized fashion enables the network's high scalability and efficient management
- Challenges:

  - security issues occur in the data exchange: device impersonation, false authentication or unreliability

  - low computational power and storage capabilities of IoT devices

REFERENCE

[1] Blockchain, https://en.wikipedia.org/wiki/Blockchain

[2] The Architecture of Blockchain System across the Manufacturing Supply Chain,Zheyi Lu, http://www.diva-portal.org/smash/get/diva2:1263343/FULLTEXT01.pdf

[3] A systematic literature review of blockchain-based applications: Current status, classification and open issues, Fran Casino, https://www.researchgate.net/publication/329136952_A_systematic_literature_review_of_blockchain-based_applications_Current_status_classification_and_open_issues

[4] Where is Blockchain Technology in 2020? , Noama Samreen, https://medium.com/the-capital/what-is-blockchain-technology-2020-712893d05ac4

[5] Blockchain Technology Ensuring Data Security & Immutability, Gautam Raturi, https://towardsdatascience.com/blockchain-technology-ensuring-data-security-immutability-7150d309352c

[6] Blockchain evolution: from 1.0 to 4.0, Unibright.io, https://unibrightio.medium.com/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666

[7] Security and Privacy on Blockchain, Rui Zhang, https://arxiv.org/pdf/1903.07602.pdf

[8] 30 BLOCKCHAIN APPLICATIONS AND REAL-WORLD USE CASES DISRUPTING THE STATUS QUO, Sam Daley, https://builtin.com/blockchain/blockchain-applications

[9] Once hailed as unhackable, blockchains are now getting hacked, Mike Orcutt, https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

[10] Database containing personal information of over 270,000 Ledger customers released on RaidForums, Aislinn Keely, https://www.theblockcrypto.com/linked/88596/database-containing-personal-information-of-over-270000-ledger-customers-released-on-raidforums

[11] Ultimate Guide To Pros And Cons Of Blockchain, Gwyneth Iredale, https://101blockchains.com/pros-and-cons-of-blockchain/#prettyPhoto

[12] Blockchain, Cryptocurrencies, and the Dark Web, Dmitry Budko, https://dzone.com/articles/blockchain-cryptocurrencies-and-the-dark-web

[13] Security and Privacy on Blockchain, https://arxiv.org/pdf/1903.07602.pdf

[14] Blockchain & Cyber Security. Let's Discuss, Deloitte EMEA Grid Blockchain Lab, https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/Blockchain-and-Cyber.pdf

Thank you!

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:30 Privacy Preserving Technologies (continued)
12:30 – 13:30 Student Presentations – Miscellaneous
- Yo-Shuan Liu – Usable Security
- Philana Williams – Security for Web App Development
- Haonan Xu – Privacy issues in Cloud Computing
- Pratishtha Singh – Card privacy Concerns in India
- Yilin Zhang - Blockchain and Data Security

13:30 – 13:40 Break
13:40 – 14:55 Class Discussion – Mass Surveillance
14:55 – 14:15 China's Social Credit Score
14:15 – 14:50 Review for Final Exam
14:50 – 13:20 Current Event Discussions

Discussion on Mass Surveilance

We will discuss views regarding issues of surveillance technologies and the integration of data from multiple sources into a unified profile/timeline for the individual.

- **Consider the various places where these technologies are deployed and how they are used?**
- **Are there similar technologies deployed commercially?**
- **What has changed about the technologies over time that make them more intrusive?**
- **What are the societal and commercial benefits that can be achieved through use of these technologies.**

Readings on Mass Surveillance

Another Netflix Viewing: Black Mirror – “Nosedive” – Season 3, Episode 1

This is fiction, but it allows one to think about the implications of rating all interactions on social media and how this becomes a means of control. If you have Netflix I encourage you to watch this episode. **This is not directly about surveillance, but it does provide a dystopian view of what happens when all of our interactions are rated by others, and how those ratings influence our behavior and our lives.**

But now on to surveillance:

Police Will Pilot a Program to Live-Stream Amazon Ring Cameras -

Matthew Guariglia -November 3, 2020

- https://www.eff.org/deeplinks/2020/11/police-will-pilot-program-live-stream-amazon-ring-cameras

Recent Reports Facial Recognition

Police are using facial recognition for minor crimes because they can - Alfred Ng – Cnet 10/24/2020

Law enforcement is tapping the tech for low-level crimes like shoplifting, because there are no limits. But the tool often makes errors.

Portland officials pass strict ban on facial recognition systems – engadget – September 9, 2020

Even private companies won't be able to use them.

In the document (PDF) detailing the ordinance, the city council noted that “Black, Indigenous and People of Color communities have been subject to over surveillance and disparate and detrimental impact of the misuse of surveillance.” It added that face recognition technologies “have been documented to have an unacceptable gender and racial bias” and explained that the city “needs to take precautionary actions until these technologies are certified and safe to use and civil liberties issues are resolved.”

Recent Reports Facial Recognition

Face for sale: Leaks and lawsuits blight Russia facial recognition

- by Umberto Bacchi | Thomson Reuters Foundation - Monday, 9 November 2020 10:03

The rise of cloud computing and AI have popularised face recognition technology globally, but at what cost?

- TBILISI, Nov 9 (Thomson Reuters Foundation) - When Anna Kuznetsova saw an ad offering access to Moscow's face recognition cameras, all she had to do was pay 16,000 roubles ($200) and send a photo of the person she wanted spying on.
- The 20-year-old - who was acting as a volunteer for a digital rights group investigating leaks in Moscow's pervasive surveillance system - sent over a picture of herself and waited.
- Two days later and her phone buzzed.
- The seller had forwarded the paralegal a detailed list of all the addresses in the Russian capital where she had been spotted by cameras over the previous month, her lawyers said.
- "It was really incredible," said Sarkis Darbinyan, a lawyer for Roskomsvoboda, the group behind the investigation. "We got a report of all her movements in Moscow."
- The incident is now under police investigation.
- Far from an aberration, the incident is at the centre of one of several lawsuits brought in recent months by rights activists against the Russian authorities over their use of face recognition.
- The rise of cloud computing and AI technologies have popularised the technology globally, with supporters saying it promises greater security and efficiency.
- But the backlash is growing, too, as critics say benefits come at the cost of lost privacy and increased surveillance.

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:30 Privacy Preserving Technologies (continued)
12:30 – 13:30 Student Presentations – Miscellaneous
- Yo-Shuan Liu – Usable Security
- Philana Williams – Security for Web App Development
- Haonan Xu – Privacy issues in Cloud Computing
- Pratishtha Singh – Card privacy Concerns in India
- Yilin Zhang - Blockchain and Data Security

13:30 – 13:40 Break
13:40 – 14:55 Class Discussion – Mass Surveillance
14:55 – 14:15 China's Social Credit Score
14:15 – 14:50 Review for Final Exam
14:50 – 13:20 Current Event Discussions

Reputation – and "credit" scores

- Toward a Reputation State: The Social Credit System Project of China – By Xin Dai – Ocean University of China.
  - In designing the SCSP, the Chinese government envisioned that reputation mechanisms such as blacklisting, rating, and scoring be used to tackle many of the country's by far intractable governance and regulatory problems in its social and economic realms, ranging from fraudulent behaviors in the marketplace, to difficulties in enforcing court judgments, to corruption in the government, and to professional malpractices and even plagiarism in scholarship. Although
- Into the Black Mirror: The Truth Behind China's Social Credit System
  - Blacklists… data… credit scores… all sensationalized elements of the Chinese policy plan regularly blasted as reminiscent of *1984*: the Social Credit System. Often compared with chilling dystopian science-fiction episodes, the topic has received breathless coverage from some members of the international media, but information is often inconsistent or saturated with alarmism. On the other hand, Chinese officials tout it as a policy that expands financial services and improves law enforcement, a position often met with skepticism due to the authorities' lack of transparency.

Readings: Reputation

- How the West Got China's Social Credit System Wrong Wired July 29, 2019.
  - But there is no single, all-powerful score assigned to every individual in China, at least not yet. The “official blueprint” Pence referenced is a planning document released by China’s chief administrative body five years ago. It calls for the establishment of a nationwide scheme for tracking the trustworthiness of everyday citizens, corporations, and government officials. The Chinese government and state media say the project is designed to boost public confidence and fight problems like corruption and business fraud. Western critics often see social credit instead as an intrusive surveillance apparatus for punishing dissidents and infringing on people’s privacy.

Readings: Reputation

- **Inside China's Vast New Experiment in Social Ranking – Wired December 14, 2017.**
  - In 1956 an electrical engineer named Bill Fair and a mathematician named Earl Isaac started a small tech company out of a San Francisco apartment. They named it Fair, Isaac and Co., but the business eventually came to be known, for short, as FICO. Their chief innovation was using computer-driven statistical analysis to translate people's personal details and financial history into a simple score, predicting how likely they were to pay back loans.

  - One day a new icon appeared on Liu's Alipay home screen. It was labeled Zhima Credit (or Sesame Credit). The name, like that of Alipay's parent company, evoked the story of Ali Baba and the 40 thieves, in which the words *open sesame* magically unseal a cave full of treasure. When Liu touched the icon, he was greeted by an image of the Earth. "Zhima Credit is the embodiment of personal credit," the text underneath read. "It uses big data to conduct an objective assessment. The higher the score, the better your credit." Further down was a button that read, in clean white characters, "Start my credit journey." He tapped.

Readings: Reputation

- https://www.fastcompany.com/3050606/china-is-building-the-mother-of-all-reputation-systems-to-monitor-citizen-behavior Fast Company - September 16, 2015.
  - "They've been working on the credit system for the financial industry for a while now," says Rogier Creemers, a China expert at Oxford University. "But, in recent years, the idea started growing that if you're going to assess people's financial status, you should equally be able to do that with other modes of trustworthiness."

- https://www.fastcompany.com/90177771/chinas-orwellian-social-credit-system-is-expanding-overseas/, Fast Company – June 28 2018.
  - A report from the Australian Strategic Policy Institute says China's social credit system will begin expanding past China's borders to monitor Chinese citizens wherever they are globally. **The system will also start applying to international companies that do business in China. As a result, the social credit system is not just shaping the behaviors of Chinese citizens beyond their border but international companies as well.** If an international business gets a low social credit score, it could lead to fines for the company, higher interest rates for loans, or even the blacklisting of its products.

- https://www.fastcompany.com/90394048/uh-oh-silicon-valley-is-building-a-chinese-style-social-credit-system
  - The most disturbing attribute of a social credit system is not that it's invasive, but that it's extralegal. Crimes are punished outside the legal system, which means no presumption of innocence, no legal representation, no judge, no jury, and often no appeal. In other words, it's an alternative legal system where the accused have fewer rights.

Corporate Reputations

The final two additional articles relate to China's "corporate social credit system". Most of our discussion has focused on the rating of citizen's, but this focuses on how a similar scoring will be provided to rank companies on their actions and statements to provide incentives and disincentives around "good" corporate behavior.

- https://www.dw.com/en/chinas-corporate-social-credit-system-spooks-european-companies/a-50200050

- https://www.europeanchamber.com.cn/en/press-releases/3045/european_chamber_report_on_china_s_corporate_social_credit_system_a_wake_up_call_for_european_business_in_china

Today's Agenda

12:00 – 12:05 Introduction and Announcements
12:05 – 12:30 Privacy Preserving Technologies (continued)
12:30 – 13:30 Student Presentations – Miscellaneous
- Yo-Shuan Liu – Usable Security
- Philana Williams – Security for Web App Development
- Haonan Xu – Privacy issues in Cloud Computing
- Pratishtha Singh – Card privacy Concerns in India
- Yilin Zhang - Blockchain and Data Security

13:30 – 13:40 Break
13:40 – 14:55 Class Discussion – Mass Surveillance
14:55 – 14:15 China's Social Credit Score
14:15 – 14:50 Review for Final Exam
14:50 – 13:20 Current Event Discussions

Friday May 7th - Final Exam

The Final exam for DSci529 will be held Friday May 7th from 11AM to 1PM PDT.

- An alternate time will be provided for those with scheduling conflicts (e.g. because of their time-zone)
- At 11AM (or an alternate time) two files will e-mailed to all students:
  - A word document with the exam
  - A text document with the exam
- You will complete the exam in word or any other text editor of your choice and upload exam to D2L Dropbox by 1:15 PM (15 minutes added for logistics, etc)
- The exam will include a self certification that you neither gave nor received any assistance during the exam.

Discussion and Review for the Exam later in Lecture

Friday May 7th - Final Exam

Exam will be open book and open note.

- You may not use your computers for communication during the exam.
- You may not visit external websites during the exam.
- Download all references before beginning the exam.

Material covered on the exam

- The exam is comprehensive
- But the emphasis will be on materials and discussion covered after the mid-term exam.
- Previous exams have been posted to http://ccss.usc.edu/529 (2020 exam will be posted this weekend)

Outline of Material Covered

- Artificial Intelligence and Bias
- Internet of Things
- Social Media
- Regulation of Content and Disinformation
- Use and Access to Data by Governments
- Privacy Regulation
- Privacy Preserving Technologies
- Mass Surveillance
- Plus material pre-midterm
  - Primarily Technical Means of Protection (including identification)
  - Also Big Data and Expectations of Privacy

Sample Exam: Spring 2020

1. Privacy and Security (50 points)

a) GDPR (10 points)
What are the most important differences in GDPR as compared with previous electronic privacy regulations? Be sure to discuss the of GDPR that makes it applicable to more activities than existing regulations. What are the activities covered by GDPR that are not covered by many previous privacy regulations?

b) CCPA (20 points)
Discuss some of the ways that the California Consumer Privacy Act will impact privacy for the rest of the United States. Discuss the specific provisions that will have an impact, and the reason that those provisions will impact consumers outside of California.

c) China's Social Credit Score (20 points)
What benefits might be provided to society from deployment of fully integrated and futuristic mass-surveillance and scoring systems such China's plans for their social credit score. What could go wrong in such a system and/or how might such a system be abused (how in terms of the method by which it could be abused, and also how in terms of the misuse that could be made of such a system).

Sample Exam: Spring 2020

2. Technologies (30 points)

a. Fairness & discrimination when processing “Big Data” (10 points)

Explain some of the ways that the application of data science and artificial intelligence to large unstructured data sets (i.e. Big Data) creates the potential for illegal discrimination. What actions can one take to reduce the likelihood of such discrimination?

b. End to end encryption (20 points)

What is meant by end-to-end encryption in applications like email (e.g. PGP), messaging (e.g. What’s App) and video conferencing (e.g. Zoom)? What potential remains in these systems for interception of communications? Why have many governments proposed limitations on or banned support of end-to-end encryption and what are some of the arguments against such bans.

Sample Exam: Spring 2020

3. Privacy in the age of Pandemics (20 Points)

It is quite common to see weakening of privacy protections and/or other freedoms during a crisis and the Covid-19 pandemic is a case in point. It is interesting to note that in the field of public health, monitoring the spread of disease and illness has always been referred to as epidemiological/disease surveillance, which highlights the intrusive nature of such monitoring. In this question you are to consider the contract tracing framework put forth by Apple and Google, as discussed in class.

a. What is Privacy? (8 points)

Discuss some of the goals for privacy in such a coronavirus contract tracing application. Specifically, what do we mean by privacy for this application… What can be done with data, who should have access to the data or conclusions, and what kinds of monitoring/tracking/inferences should be prevented? Note that for some parts of this answer there might be more than one legitimate point of view, and you should discuss both points of view where appropriate.

b. Privacy Preserving Features (5 points)

What are some of the features of the Google/Apple proposal that tend to improve certain aspects of privacy as outlined by you in part (a).

c. Privacy problems (7 points)

List a few ways that someone could exploit the data collected by the app to violate the security policies descried in part (a). Suggest steps that could be taken/changes to be made that could reduce the impact of any of the breaches you just described.

Current Event Discussion

- http://csclass.info/USC/INF529/s21-lec14-ce.html