Cybersecurity for Future Presidents

Lecture 7:
DEBATE #2:

Debate 2: Resolved: The US should adopt the E.U. “right to be forgotten” online.
Any Questions?
- About previous lecture?
- About homework? (debate questions)
- About reading? (D is for Digital Chapters 3, 11; debate articles and videos)

Midterm this Friday!

Reading for next week (after midterm): D is for Digital, Part III, Communications, introduction and Chapter 8, pp. 117-134.
Exercises: based on the reading.

Next Debate (in 2 weeks): Resolved: The U.S. Election Assistance Commission should promote internet voting for public elections on a model similar to Estonia.
Debate teams please sign up to see me this week or next week.
Cybersecurity events from the past week of interest to future (or current) Presidents:

While you were out...

• U.S. DoJ readies indictment of 5 Iranian hackers for 2013 attempt to control Rye NY flood control dam

• $81M theft from New York Fed via malware on Bangladeshi computers - stolen credentials. Further transactions caught via human detection of spelling error

• South Korea energy, transportation, other infrastructure industries hit by “OnionDog” attacks over past 2 years

• Apple - FBI dispute continues to simmer in public press

• Dept of Justice said to be eyeing similar action against WhatsApp (encrypted messaging)

• Happy Madison’s Birthday! Author of Bill of Rights.

Coming up: ... ?
Today’s Debate Topic

Debate 2: Resolved: The US should adopt the E.U. “right to be forgotten” online.
What we’ve covered so far - Readings

Texts:
• Kernighan, D is for Digital: Preface, Chapters 1-3 and 10-11
• Anderson, Security Engineering: Chapter 1, pages 3-15

Other
• Clark, Berson, Lin, At the Nexus of Cybersecurity and Public Policy: Tensions between cybersecurity and other public policy concerns, pp. 93-115.
• Abelson et al: Keys Under Doormats
• Landau, Making Sense of Snowden
• Vance, Report on Smartphone Encryption and Public Safety
• US-CERT, Understanding Web Site Certificates
• EU factsheet on the Right to be Forgotten
• Toobin, “The Solace of Oblivion”
What we've covered so far, Lectures

Technology topics

- Cybersecurity terms and issues, Digital vs. Analog, Information vs. Data, data representation, bit manipulation
- Basic computer architecture
- Basic Telephony (circuit switching vs packet switching)
- Cryptography history and technology, bit operations symmetric vs asymmetric crypto
- Cybersecurity fundamentals: system security, access control, C.I.A. properties, Policy, Mechanism, Assurance, Incentives
- Cyberattacks: DoS/DDoS, Attacks via inputs (B.O.), Supply Chain, Side Channels, Social Aspects

Policy topics

- US Government Structure
- Search and surveillance history, legislation, court cases
- Cryptography policy and legislation
- Privacy Fundamentals: FIPPs, U.S. vs. E.U. policy approaches; Safe harbour, Right to be forgotten

Critical Thinking: Debates #1 and #2
Another way to understand buffer overflow attacks, if you use the web:

• Imagine you click a hyperlink on a web page.
• Your browser knows the page you are currently on and saves its location so when you press “Back” you can return there.
  - Your browser translates the first part of the URL to an IP address via DNS
  - Sends request to the IP address and retrieves a page, which may include Javascript programs that execute within your browser
  - Suppose that Javascript overwrites the place where your browser saved your “Back” address with some other page.
  - Now you press the “Back” button and you end up on some other page entirely
• This is similar to what happens in the buffer overflow attack: you end up executing a program (vs. viewing a web page) that is other than what you intended.
Yet Another way to think about what happens in a buffer overflow, if you enjoy cooking

- Suppose you are cooking something from a recipe with several sub-parts
- You start following the directions, setting a bookmark each time you go to a different page so you can find where to return

Page 471:
Chicken Supreme Papillote
1. Preheat oven to 400°F.
2. Prepare: Breast of Chicken, allowing it to cook until ½ done. Place it on a parchment heart for Papillote, → page 131.
3. Before folding, place: 1 Tablespoon Colbert Butter, → page 339, on each ½ breast. Seal the paper and bake on a baking sheet for about 15 minutes.
4. Serve with: Pilaf, → p. 183

Page 131:

Page 653: Brownies
1. Melt ½ C. butter and 4 oz. chocolate, and let cool.
2. Beat 4 eggs with ½ tsp. salt.
3. Add 2 C. sugar and 1 tsp. vanilla
4. Combine chocolate, eggs, and sugar.
5. Fold in 1 C. sifted flour and stir in 1 C. pecans
6. Bake in 9” x 13” pan at 350°F. about 25 minutes.
What is yet to come …

- Accountability, including identification, authentication, forensics
- History of computer security policy/economics
- Elections and cybersecurity
- Genomics and cybersecurity
- Digital currency technology and policy
- Issues for future presidents
<table>
<thead>
<tr>
<th>Criteria</th>
<th>20</th>
<th>15</th>
<th>10</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Addresses Issues</strong></td>
<td>Always addresses topic</td>
<td>Usually addresses topic</td>
<td>Rarely addresses topic</td>
<td>Did not address topic</td>
</tr>
<tr>
<td><strong>Support with Facts</strong></td>
<td>Uses many facts that support topic</td>
<td>Uses some facts that support topic</td>
<td>Uses few facts that support topic</td>
<td>Does not use facts that support topic</td>
</tr>
<tr>
<td><strong>Persuasiveness</strong></td>
<td>Arguments clear and convincing</td>
<td>Arguments are sometimes clear and convincing</td>
<td>Arguments are rarely clear and convincing</td>
<td>Arguments are never clear and convincing</td>
</tr>
<tr>
<td><strong>Writing</strong></td>
<td>Clear and concise</td>
<td>Mostly clear and concise; Few minor flaws</td>
<td>Somewhat clear and concise; Many minor flaws or a major flaw</td>
<td>Not clear and concise; A few major flaws</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td>Structure is logical; Transition sentences help connect topics; Progression of ideas evident</td>
<td>Structure is logical but a bit faulty; Transition sentences may be missing for a few topics; Progression of ideas exists but a bit faulty</td>
<td>Structure is partly logical and partly random; Transition sentences may be missing for a few many topics; Progression of ideas exists but faulty</td>
<td>Structure is mostly random; Transition sentences are lacking; Progression of ideas does not exist</td>
</tr>
</tbody>
</table>