Mid-Semester Project - Encryption

Due: Wednesday, April 13 2016

11:59 PM, Submit On Canvas

Partner Project

Required total length: 4300-5400 words
January 27th, 2017
TFEC Headquarters
115 Waterman Street
Brown University
Providence RI, 02912

Dear Members of the Task Force on Encrypted Communications,

The President has taken the oath and we at the White House are eager to begin the effort to translate our campaign promises into reality. Polls show that America's number one fear is the Islamic State, and their defeat is our first priority. I received word this morning that your task force has officially obtained Top Secret clearance. In accordance, I am attaching intelligence briefs that our agencies have compiled. They demonstrate that the Islamic State's familiarity with cryptography has enabled them to blind our government to their communications. Since the tragic shootings in San Bernardino and Paris, their ability to conduct secret communications has continued to hinder our fight.

In response to recent events, the Speaker of the House and Senate Majority Leader have drafted a bill, with bipartisan support, to outlaw our strongest systems of encryption. The law includes measures to compel companies to provide the government with backdoors, to force any firm that offers secure communications to break it with reasonable suspicion of terrorist
usage, and to limit our nation's researchers' ability to construct stronger encryption and to
document their cryptosystems in a public form. The President is hesitant. We know, however,
that Congress can pass this bill over a veto and that a veto may be political suicide.

That is precisely why we have assembled you. Your team represents our nation's
brightest minds in computer science and technical policy. We need you to draft an alternative
plan that our administration can adopt to solve this crisis. We need the plan to include three
components. We need a piece of legislation that the President can introduce to Congress to
replace their plan. We need a draft committee report justifying any changes. And we need the
plan to include any executive orders that the President has the authority to issue as well as any
directives to the executive branch or armed forces of the United States. I want to reiterate the
importance of your dual skills as computer scientists and policymakers. We do not want you to
spare a single technical detail in any of these documents. We need an air tight set of legal and
technical documents. These combined need to meet be at least 4300 words but no more than
5400 words not including the bibliography.

You have until April 13 2016 (yes we are traveling backward in time!).

Good luck. Your country needs you.

Respectfully submitted,

[Signature]

John Savage
Secretary of Technology
The White House
Washington D.C.
PRESIDENTIAL BRIEF

Our intelligence systems are going increasingly dark as terrorist networks continue to distribute information about using secure communication technologies. Right now the Central Intelligence Agency is most successful when we intercept communication from an actor who implemented a cryptosystem incorrectly. We request assistance from the White House via permission to compel firms to cooperate with the agency’s attempts to break the security of known radicals or radical sympathizers’ accounts. Please see the attached breakdown of messaging technologies which we intercepted from a terrorist cell operating out of Islamabad, Pakistan. In addition, we are seeing an increasing presence of GPG and other hand rolled cryptosystems among radical groups. The agency cannot continue to be effective without authorization from the President.

Another critical concern is that terrorist networks, particularly groups aligned with the Islamic State, are utilizing communication technologies that are ancillary to a product’s main purpose. For example, raids are revealing an increasing number of Sony Playstations and Microsoft Xboxes. We believe that these organizations are using the chat services in video games to communicate and plan attacks. These communications are extremely difficult to intercept especially without the assistance of their creators. This is an opportunity for the White House to establish the relationships with companies that are reticent of work with the intelligence agencies. The fact that the majority of individuals communicating across these channels are American citizens and the way that games group these messages puts the security agency in a precarious legal position for bulk collection.

When military or intelligence officers detain an enemy combatant, the officers are trained at capturing the target’s phone before the suspect could destroy it. Recently combatants no longer fear capture of their devices since they are encrypted using today’s highest standards. Apple iOS devices are not actually the concern that the media raises given their relatively small password size and the intelligence community’s skill at touch wear analysis to crack the password when detainees do not surrender it. Other devices have become intractable to crack given our enemy’s widespread knowledge on secure password construction. These devices will become a terrorist network’s best weapon if this administration does not authorize us to force companies to aid in cracking or ban the use of these encryption standards without a backdoor.

An ongoing struggle for all U.S. intelligence organs is the difficulty of recruiting qualified agents with strong computational expertise. Technology firms are able to offer more than triple our base salary and present additional perks that are not in accordance with military life. We are losing our technical edge and need policy
changes to ebb our brain drain. We need the ability to recruit America’s best computer security talent.

Please see the included intercepted intelligence materials to better understand the state of the art in radical groups’ encryption and computer security standards.

SPECIFICATION

SUMMARY

This is a partner project; two students, no more and no less. The course staff recommends that you pair CS expertise with policy expertise but this is not required. You are welcome to divide the 16-20 pages between these sections as you feel necessary but do not use this leniency to neglect any section. Each part will be graded individually as well as overall.

We do not require that each part fulfil any particular length, as long as you include each part in your final submission. The total length, however, should be between 4300 and 5400 words - that’s the same as about 16-20 pages double spaced (Note that this is the SAME length as the Critical Infrastructure midterm, but that one is specifically divided into 2 parts so the word counts are divided by two in the assignment handout.

PART 1: LEGISLATION

This part of the project represents an opportunity to truly practice your technology policy skills as well as work on the clarity and specificity of your writing. Although your proposed legislation does not need to meet the exact style of a United States House or Senate bill, nevertheless the wording should be precise enough that legislative assistants would be able to convert it into a bill without a loss of meaning or need for further clarification. The text of the legislation should not focus on justifications for your changes; these justifications should be included in the committee report. You may advocate for any legislative approach to this issue, from strict requirements on technology companies to enshrining the right to secure and private communications as a fundamental belief of the United States. The TA staff will be evaluating your ideas with metrics of coherence, structure, and fullness.

PART 2: COMMITTEE REPORT

In the committee report, you will argue for your plan and justify any proposed legislative changes from both policy and technical perspectives. Be sure to include a discussion of both; committee reports that deal only with policy justifications without discussing technical issues will be penalized, and vice versa. This section will provide you with practice in persuasive communications, and the TA staff will evaluate the persuasiveness of your argument. Be sure to include opposing positions and critique counterarguments. Your legislation and committee report must maintain a consistent position with individual components aiding a global theme. It cannot leave any question unanswered.
PART 3: EXECUTIVE ACTIONS

The Executive Actions must meet the same requirements as the proposed legislation, but should focus on direct actions as opposed to policy and legal questions. These actions can include policy changes through executive action, or other presidential actions. For instance, President Obama recently signed an agreement with President Xi Jinping of China prohibiting cyber espionage for economic gain.

The first part presents the United States’ long term strategy, ideology, and the values that the country wants to hold itself to and its companies to. This part represents what your group believes the President and various executive agencies should do in the short term. This part should contain intelligence and military strategy relating to this problem. The TA staff will look to ensure that your short term strategy enables your long term strategy, that the actions you want to undertake are arguably constitutional as executive action, and that you are directing the executive branch in a comprehensive manner. The TA staff will evaluate your writing in a similar manner as before since both legislation and executive orders must have utmost clarity, specificity, and purpose.

WRITING

As consistent with the course missive, all pieces of writing must meet the guidelines of the Elements of Style handout. In addition, you must use proper spelling, punctuation, and grammar.

DESIGN CHECK

Note: The design check is now OPTIONAL. We highly recommend coming to hours to discuss your design, but we will not deduct points if you choose not to.

If you do choose to come to hours for a design check, it would help us if you bring a bullet point outline of your ideas for each section to a fifteen minute conversation with two TAs. You do not need to prepare any written material but you are certainly welcome to. You must have enough to discuss your proposals for fifteen minutes. This an opportunity to have TAs challenge your ideas and work through any concepts that you struggle with so the more you prepare, the more benefit you will reap.

GRADING RUBRIC

**Please note that we will grade you directly from this rubric**

<table>
<thead>
<tr>
<th>Paper Guidelines (100 Points)</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td></td>
</tr>
<tr>
<td>Long Term Policy Solutions (Legislation)</td>
<td>10</td>
</tr>
<tr>
<td>Long Term Technical Solutions (Legislation)</td>
<td>10</td>
</tr>
<tr>
<td>Justifications for Long Term Policy and</td>
<td>20</td>
</tr>
</tbody>
</table>
Technical Solutions (Committee Report)

<table>
<thead>
<tr>
<th>Short Term Proposal (Executive Action)</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justification for Short Term Proposal (Executive Action)</td>
<td>10</td>
</tr>
<tr>
<td>Counterargument</td>
<td>15</td>
</tr>
<tr>
<td>Writing &amp; Style</td>
<td>25</td>
</tr>
</tbody>
</table>

Things to think about:

Writing is inherently subjective and grading written work is difficult but we will provide you with our guiding framework.

1. Feasibility – are the ideas discussed technically and legally feasible? Does the work ground its ideas in known facts and establish its own feasibility? The particular positions you take do not matter. A logically argued and well written essay the TAs do not agree with will receive a higher grade than a poorly written essay we do agree with.

2. Coherency – does the work make sense as a coherent piece at the overall and sectional level? Does every piece complement rather than contradict each other?

3. Landscape – does the work demonstrate an understanding of the legal and technical precedent? Does it acknowledge and dispute counterarguments?

We encourage you to consider this framework as a minimum and to strive to exceed expectations. This project is open-ended and allows for creativity. It is difficult to describe in a rubric but easy to identify as graders the difference between well researched work and surface level work. We will be rewarding heavily the former.

EXAMPLES:

1. Legislation
   a. DOTCOM Act of 2015
      i. [Text of the Legislation](#)
      ii. [Committee Report](#)
   b. Cybersecurity Information Sharing Act of 2015
      i. [Text of the Legislation](#)
      ii. [Committee Report](#)
   c. Cyber Intelligence Sharing and Protection Act
      i. [Text of the Legislation](#)
      ii. [Committee Report](#)

2. Relevant Committees
   a. Senate Homeland Security and Government Affairs Committee
b. Senate Foreign Relations Committee (particularly the Subcommittee on East Asia, The Pacific and International Cybersecurity Policy)
c. Senate Select Committee on Intelligence
d. Senate Commerce, Science and Transportation Committee
e. House Committee on Foreign Affairs
f. House Homeland Security Committee
g. House Committee on Oversight and Government Reform
h. House Committee on Science, Space, and Technology
i. House Permanent Select Committee on Intelligence

3. Executive Action
   a. Presidential Memorandum on the Establishment of the Cyber Intelligence Integration Center
   b. Executive Order Improving Critical Infrastructure Cybersecurity