Digital Security for Lawyers: A Proposal for the Information Society Project at Yale Law School

Sean O’Brien
Yale University

Statement of Intent

As a Visiting Fellow at the Information Society Project, I will provide digital security expertise for law students, lawyers, and legal professionals. I will produce a guide to software security, privacy, and anonymity tools, with the working title “Digital Security for Lawyers” (hereafter DSL). DSL will introduce tools and techniques that are standard in the digital security industry, as well as emerging and “bleeding-edge” software. DSL will be loosely modeled after Susan McGregor’s pioneering handbook for journalists and, likewise, will provide a framework for further discussions, lectures, and workshops around these topics. There is a keen interest in digital security and private communication amongst the general public, and alarming breaches at law firms have reinforced the need for technology training in the legal profession.

1 Background

Digital security practice has changed substantially in a short time. The considerable and increasing trend of cyber attacks, data breaches, leaks, and software vulnerabilities shows no signs of abatement. Legal professionals are presented with emerging challenges to the practice of law, especially where confidentiality and data integrity is concerned. Traditional approaches to legal education and practice do not address these concerns, even as technology becomes more central to standards of professional conduct. Lawyers are increasingly expected to “keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.” Lawyers must also “make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client”.

2 Topics Covered

DSL will introduce cryptography, networks, and digital security concepts, while staying grounded in the central security concept of trust. DSL will recommend software to the reader that is built around a web of trust model, as well as tools designed to obfuscate or mask user identity on computer networks. There has been a dramatic growth in the development of privacy, security, and anonymity software in the past year, an effort owing most to the fallout from the Snowden disclosures. Of the many options available, DSL will recommend free/open-source software (FOSS) programs. FOSS is preferred by security researchers and penetration testers, and FOSS programs consistently top the list of secure, privacy-respecting tools available.

DSL will briefly describe the community-development model of FOSS, as well as the licenses that identify programs as free or open-source software. Beyond the legal importance of this topic, lawyers who can correctly identify the type of software they are using will be better able to identify malicious and untrustworthy programs and improve their security practice. DSL will explain some of this software, offering a quick guide to tools such as the Tor Browser Bundle, Crypto.cat, and Enigmail. These examples provide simple and friendly interfaces for technology which might typically be considered arcane and exotic. Where mobile devices are concerned, lawyers would benefit from the usage of private messaging apps, such as those available from the FOSS “app store” F-Droid, as well as those distributed by Silent Circle.

3 Relevance

The relevance of digital security goes beyond personal communication and data handling, and is of interest
to anyone studying our Information Society. FOSS powers much of the Internet and is vital to the most widely-installed operating systems in the world. Lawyers working with high-profile clients will need security training, and a solid guide to widely-available tools will be indispensable.

The increasingly-hostile nature of network actors makes solid operations security (OPSEC) a requirement if confidentiality will be maintained at all in the 21st Century. As a guide to better digital security, DSL will prepare lawyers for changes that are occurring in the global software ecosystem, a transformation that will not doubt continue.

The ABA has formed a Cybersecurity Legal Task Force, with ambitious goals and new guidance for data and communications security. Without security training, this guidance may seem inundating. A simple handbook, with specific software recommendations and action items, will be welcomed by the legal community and further cement ISP’s role as a leader in regard to technology issues.

4 My Role as Visiting Fellow

My professional work, as well as my personal interests, makes me uniquely-poised to advise ISP on security practice. I have been working in higher education for 13 years, in academic support positions as well as system administration. Throughout my career I have been responsible for protecting confidential data, which has included biographical, academic, financial, immigration, and employment records. My duties have ranged from technical support to web development to database administration, and I have created both server-side and web-based solutions to collect data for large enterprise applications. Proactive security practice has become essential in my profession and, in the past two years alone, I have faced hostile threats to my servers as well as zero-day vulnerabilities that required my full and immediate attention.

Beyond this work as a sysadmin and developer, my history with the FOSS community will provide ISP with valuable insight into our digital world. Global FOSS collaboration is the engine that drives our digital era, having increased both the pace of technological growth as well as its ubiquity. My friends and colleagues at the Free Software Foundation, Red Hat, Debian, the Berkman Center, and their international counterparts comprise a loose-knit social network that is on the cutting-edge of the evolving tech landscape.

As an Educational Technologist, I have facilitated a series of workshops and discussions around FOSS and digital security issues, most recently at Yale Law School. I am currently planning more workshops with community groups in Connecticut and New York, including MakeHaven, OpenHatch, and OpenITP. ISP would benefit from links to these groups, and could position itself as a hub of software security discussions. As security practice becomes more central to the legal profession, ISP will be a leading voice in the conversation.

Notes

1 See PRISM Break, Tactical Tech, and my own resource Get Libre for examples.
2 See the Oct. 2014 Gallup report “Hacking Tops List of Crimes Americans Worry About Most”.
3 Breaches at top law firms go back to at least 2009, when the FBI issued an advisory noting “noticeable increases” in attacks on law firms. In the past five years, such hostility has become commonplace.
4 Corporate examples include JP Morgan Chase, Home Depot, and Target, to name a few.
5 Most recently, the devastating Sony attack and its purported link to state espionage.
6 See new commentary to Rule 1.1 of the ABA Model Rules of Professional Conduct.
7 See ABA Model Rule 1.6(c), on the confidentiality of client communications.
8 The web of trust concept was first used to refer to PGP/GPG, but is also a metaphor for the structure of other implementations.
9 See PRISM Break, Tactical Tech, and my own resource Get Libre for examples.
10 For example, the EFF’s “Secure Messaging Scorecard”.
11 See new commentary to Rule 1.1 of the ABA Model Rules of Professional Conduct.
12 See ABA Model Rule 1.6(c), on the confidentiality of client communications.
13 See the Free Software Definition and Open Source Definition for descriptions of FOSS.
14 See the Oct. 2014 Gallup report “Hacking Tops List of Crimes Americans Worry About Most”.
15 See new commentary to Rule 1.1 of the ABA Model Rules of Professional Conduct.
16 For example, the EFF’s “Secure Messaging Scorecard”.
17 See the Oct. 2014 Gallup report “Hacking Tops List of Crimes Americans Worry About Most”.
18 Silent Circle was founded by PGP creator Phil Zimmermann, in an effort to develop a secure Blackphone handset using a modified version of Android. The apps for this handset, such as Silent Text, are now also available to other Android users.
19 FOSS projects Apache and nginx power over 80% of Web servers.
20 Android and its variants, which are mainly FOSS with some proprietary code, are installed on at least one billion devices with a projected 358 million more Android devices shipping in 2015.
21 Jesslyn Radack, attorney for NSA whistleblowers Drake and Snowden, has been helped by security experts to keep her communications private. I intend to make such help more accessible to lawyers.
22 By “network actors” I am referring to corporations and governments, as well as groups like Anonymous and LulzSec. Traditional institutions are now mounting cyber offenses, not just defenses.
23 OPSEC is military jargon for a process of guarding critical information, which now applies more generally to data security.