Turning the World Upside Down, or Threat Modeling a Constitution

Hi!

We're all used to a pretty wide variety of interactions with law, but it's usually about how the law affects the security world, whether it's about crypto rights, disclosure law, jurisdiction, or just not getting busted. That said, it's really rare to think about the other direction, about the security of law.

To explain what I mean, a brief digression into 17th century legal history.

The law is always a set of compromises, driven as much by competing interests as by any kind of rationality. There are, however, a wide variety of legal traditions; Roman law, in particular, attempted to build a rational framework underneath law. In his off time from developing the calculus, Leibniz picked this thread up again in the 17th century, and founded what was called the "geometrician" tradition of jurisprudence. In his Corpus Juris Reconcinnatum, he began an attempt to build a new way of thinking about the law. This tradition ultimately helped to reform much of the medieval law of Europe, opening the way for legal arguments based on deductive logic. However, the project was ultimately a failure, at least by Leibniz's standards.

Law today is still a morass of special cases, exceptions, unclear language, and often surprisingly fuzzy thinking. It's very hard to do meaningful analytic work on it, because in order to do so, you have to tackle the entire problem. The English language is far more nuanced and expressively dense, character for character, than any programming language, and just, for instance, the U.S. Code contains some tens of millions of words.

Why, then, given this complexity and the fact that the entire legal profession already exists to try to manage this beast, should hackers have anything to se about all this, outside of our own particular interests?

In part, hubris, and in part because we can, but also because in the end, systems are systems, and the tools we use to attack or defend any other system of code are just as useful for the law. In this case, our tools are threat modeling, design review, and static analysis. Maybe someday we'll expand this to include pen testing and honeypots, but we're not there yet.

This mindset, by the way, the understanding that all systems can be analyzed using similar tools, turns out to be extremely powerful -- I highly recommend taking a look at the world with it in mind and seeing what kind of trouble you can get into.

So, Iceland. Iceland is a beautiful and fascinating little country. Iceland also has a smoking hole where its economy used to be, and as a result, they've been making a few changes. In 2010, they began the process of replacing their constitution. First, a National Forum was convened, where they picked a thousand Icelanders of voting age at random, by lottery, stuck them all in a room, and asked them, roughly, what kind things they cared about being in the new constitution. Then, they held a round of elections, where about 500 people ran for a 25 seat Constitutional Assembly.

There were various wacky hijinks involving a court case, threats of a second election, etc., but the Assembly finally took their seats in May and began work on the new document. They've been working via an agile process, where the three teams within the assembly do week-long sprints, working on different parts of the document and integrating their work. Originally, they were planning on having a completed draft by this weekend with two weeks of polishing, but like any project, they're running a bit late because development is taking longer than they'd allowed; they're shooting for the end of July now. As they work, they're posting the results of each week's sprints online and taking comments, both via a specific message board and via FaceBook.

Icelandic law is interesting because they take the proposition that an individual should be able to defend themselves in court very seriously. Unlike in the US, the literal interpretation of legal text takes priority over historical interpretations. In the context of the construction of a new constitution, this means that the details of language and the logical structure of the document take on a paramount importance. The law becomes more self-contained and more code-like.

This is great from our perspective as people who want to do systems analysis; even better is being able to start fresh, and consider the constitution as a self-contained document, separate from any larger body of law.

My involvement in this whole story starts with meeting Smári McCarthy in a Thai restaurant in Reykjavik last October while hideously sick and spending a few hours rambling about security and the threat modeling work I was doing. In December, as the process was getting more seriously underway, we spent a few days working out a plan. Once the Assembly finally got down to work, so did we. There've been some hiccups along the way -- imagine trying to do a code audit of APL were all the keywords are in a language you don't speak, while trying to build the organizational framework for the project at the same time, mostly remotely, and you've got a good picture of what it's been like, but we're moving forward now. I should stress that although we know many of the members of the assembly and are working fairly closely with some of them, this is, technically, an entirely unaffiliated, amateur project. There are roughly four branches to the work we're doing.

First, we're crowd-sourcing a translation of the entire document. In a way, this is my fault, as most of the other people tangentially involved in the process speak some Icelandic, but it's also bringing a lot more external visibility. While all of our analytic products are presented in Icelandic first, we'll get all of them online in English too eventually, and hopefully get the constitution translated to maybe Spanish, Greek, and Arabic, to pick a few languages at random.

Second, we're doing a few different kinds of textual analysis:

Readability indexing uses a set of algorithms to determine the complexity and reading level of a text; we've done this on the English translation and we're working on getting the algorithms working for Icelandic. Readability is important because it's critical that a document like a constitution should be understandable by everyone in the country, clearly and easily.

We've done some simple manual checking, looking at weasel words and odd word use choices, pointing out places where the interpretation of a statement may be ambiguous.

Similarly we're looking at the Boolean logical structures of each sentence, looking for contradictions or overly complicated constructions.

We're doing unbound variable checking, in exactly the way a compiler would – finding all of the terms that are referenced in the document but never defined; the current draft has 19 or so constructs which are never defined and are not unambiguous from common Icelandic usage.

At a slightly higher level, we're looking for all of the statements which appear ambiguous from a simple common-sense reading; this shades into work of a more design review sort; more on it in a minute.

The last form of textual analysis we're looking at is deconstructing the entire document into a set of predicate phrases -- every time the document says "X shall be guaranteed Y", for instance, and looking at the implication structure between these predicates and their precedence as noted in the document.

The third large category of work we're doing is a basic design review – the same thing you do when you get a bunch of people sitting around a table trying to figure out how a system can fail. It's not perfect, but it's fast and expedient.

Finally, we're working on constructing a formal threat model of at least parts of the constitution -- this is the work I've been taking up. This is built around the work that I've been doing on threat modeling with Brenda, who spoke earlier, as part of the Trike project, and is the most direct application of computer security techniques to the law.

Trike is a tool for building formal models of processes and their implementations. Usually, these are business processes and the software systems which implement them, but any system which involves defined actors and assets that those actors care about can be modeled equally easily. Any complex adversarial process will generally reveal things when threat modeled that would not be found by having a bunch of smart people sitting around thinking about it -- the point of the technique is to enable smart people to be smarter by helping them keep track of all of the different parts of the system and what each part implies in relation to all other parts in a structured manner. You saw a bit of this earlier when Brenda spoke about data validation -- building a model of what you can and can't trust gives you a much better perspective on what you need to validate.

Of particular concern, based on the issues Iceland has faced in the past few years and based on the output from the National Forum, is a review of how the separation of powers is constructed between different branches of the government. I'll close with one bug that we've found so far.

The new constitution specifies a relatively normal three-branch parliamentarian government (Iceland all-but invented the form; the Alþingi is roughly a thousand years old), with different checks and balances between each branch. The Supreme Court has seven members usually, but in specific circumstances, another eight members are to be chosen by parliament. As in the US, the judiciary checks the combined power of the legislative and executive branches by ruling on the constitutionality and consistency of laws passed by the other branches. Unfortunately, as of the current draft, one of the instances in which the size of the court is supplemented is when the court rules on the constitutionality of legislation. This is a pretty obvious example, but it neatly encapsulates the kind of problems the threat modeling process is trying to find.

If you'd like more information about the analysis project, our wiki is here:

- http://wiki.stjornarskrarfelagid.is/index.php/Main_Page

And for more information on the Trike threat modeling methodology, see here:

- http://octotrike.org

Thanks to:

- Brenda Larcom
- Smári McCarthy
- Constitutional Assembly Members Katrín Oddsdóttir, Vilhjálmur Þorsteinsson,
- and Finnur Magnusson
- Jón Eðvald
- Tómas Árni Jónsson
- Gunnar Hólmsteinn
- Herbert Snorrason
- Clara, Ltd.
- International Modern Media Institute

Eleanor Saitta / @dymaxion

July 18, 2011 / Seattle, WA