For Good Measure

Patent Activity as a Measure of Cybersecurity Innovation

DAN GEER AND SCOTT GUTHERY

Dan Geer is the CISO for In-Q-Tel and a security researcher with a quantitative bent. He has a long history with the USENIX Association, including officer positions, program committees, etc. dan@geer.org

Scott Guthery holds over 50 patents for his work in cybersecurity. He worked for Bell Laboratories, Schlumberger, and Microsoft and co-founded Mobile-Mind with Mary Cronin to build secure mobile applications for the GSM SIM. He currently runs Docent Press, which publishes books on the history of mathematics, computing, and technology. sbg@acw.com

Country	Oldest	Newest
Belgium	5	
Canada	4	
China	7	76
Denmark	1	
EU/WTO	8	1
Finland	2	
France	8	
Germany	9	
Great Britain	7	3
Japan	4	2
Korea	1	
Netherlands	2	
Spain	4	
United States	38	18

Table 1: Country sources are consolidating geographically

Type "cybersecurity" into Google Patents, sort by oldest and then newest, and take the top 100 in each list. Keeping in mind that the lists include applications as well as grants, Table 1 lists the number of entries by country in the respective lists.

The top three assignees in the oldest list were AT&T/Bell Labs, Computer Security Corporation, and Westinghouse Electric in that order. The top three assignees in the newest list were two Chinese companies, and then IBM.

But what, you might ask, does this have to do with computer security metrics?

If you come up with a new and improved espresso machine and you wish to derive the maximum economic benefit from your invention, the two most frequently used methods of protecting your newly hatched intellectual property are applying for a patent or treating what is "new, useful, and non-obvious" in your espresso machine as a trade secret. If Table 1 were about espresso machines, the difference between the oldest and newest columns could reasonably be attributed to more companies selecting trade secret protection rather than applying for a patent.

That explanation is not as compelling for cybersecurity. A trade secret is "not generally known or reasonably ascertainable by others," but while it is possible that an innovation in cybersecurity is intended for use only within a (trade) secret context, this is not the typical business case. (This may well be the typical case in governmental and military contexts.) Because of the computer security community's aversion to secret sauce, if the inventor wishes to offer the invention in the cybersecurity marketplace, maintaining the protection of a trade secret becomes problematic; an enterprise you'd like to convince to license your innovation will want to know how it works, so protection leans more toward applying for a patent than toward using a trade secret as it would for that espresso machine. If you are going to be forced to reveal the inner workings of the invention in patent application detail, then you need to apply for a patent.

But still you ask, what does this have to do with computer security metrics?

Bruce Schneier is quoted on the Wikipedia page about elliptic curve cryptography patents ("ECC Patents") as saying in 2007, "Certicom certainly can claim ownership of ECC. The algorithm was developed and patented by the company's founders, and the patents are well written and strong. I don't like it, but they can claim ownership." Other companies hold patents on various cryptographic algorithms; the RSA patents come easily to mind.

More than a few standards discussions have wrestled with the inclusion of patented technology. Commercial entities holding a patent in such cases have every incentive to come to *fair, reasonable and non-discriminatory (FRAND) terms* for the use of their technology and thus for its use in a standard. Such was the case with both ECC and RSA. But this incentive is lacking when it is a governmental or regulatory entity that holds a patent. In this case the use of the patented technology can be required independent of any standards deliberations and in what may be very unFRANDly terms.

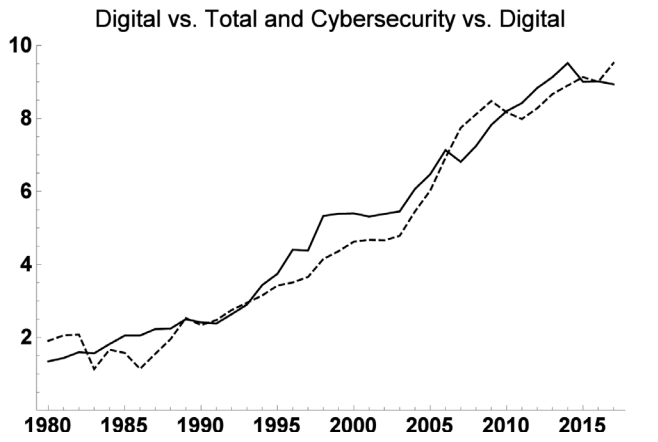

Figure 1: Digital patents as percentage of total number patents (solid) and cybersecurity patents as percentage of digital patents (dashed). All figures were drawn using data from http://www.patentsview.org/.

"OK," you say, "I do care about the computer security landscape and who owns what plots of land, but this is more about the business of cybersecurity than about the bits and bytes. Do patent numbers have anything interesting to say here?"

Here are some words that appear in the titles of the patents in the newest list that don't appear in the titles in the old list (in alphabetical order):

anti-theft, attack, authentication, detection, methods, threat, uncloneable

And here's the other way around, words in the old list titles that aren't in the new list titles:

automatic, electric, filter, lock, switch, signals, transponder, telephone

Nothing certain can be deduced from this small sample, but one can glimpse a shift away from hardware toward protocols as well as a shift from offense toward defense.

Focusing now on granted US patents from 1980 to 2017 and, in particular, on the subset of these that have the word "computer" or "network" in the patent abstract, we will refer to this subset as digital patents. Within the set of digital patents, we will distinguish those whose abstract contains at least one of a list of cybersecurity words; we will refer to these as cybersecurity patents.

Figure 1 plots by year the ratio of the number of digital patents to the total number of patents issued (solid) and the ratio of the number of cybersecurity patents to the number of digital patents (dashed). One takeaway is that roughly speaking there is as much effort going into cybersecurity innovation within the domain of computers and networks as there is going into computers and networks overall.

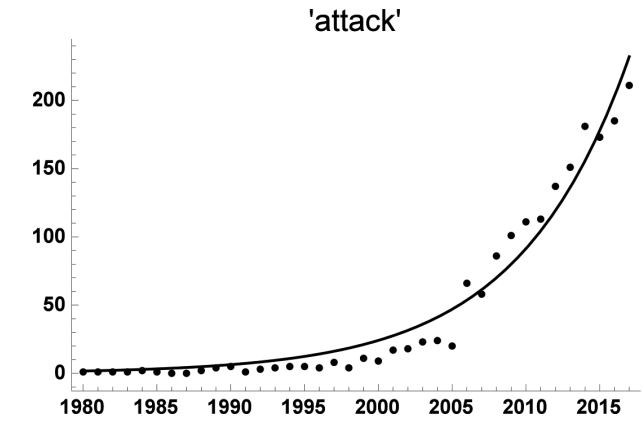

Figure 2a: Digital patents with "attack" in the patent abstract

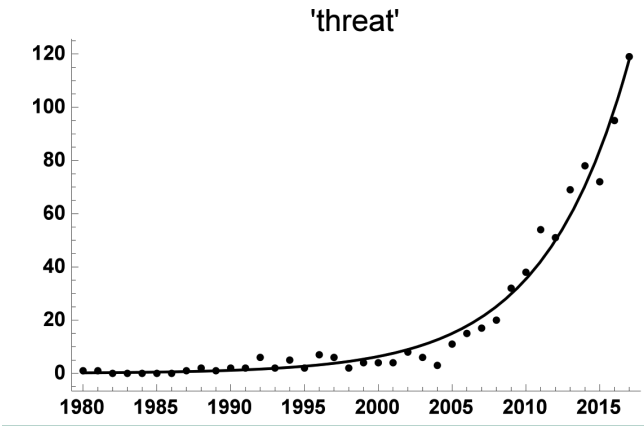

Figure 2b: Digital patents with "threat" in the patent abstract

Figures 2a and 2b plot by year the number of digital patents that have "attack" or "threat," respectively, in their abstract, together with an exponential fit to these counts.

If these plots were simply measuring the intensity of concern regarding attacks on and threats to computers and networks, then the exponential fits wouldn't be at all surprising. But they are measuring the number of "new, useful, and non-obvious" counters to attacks and threats which, in a world that might be thought of as settling into a day-in-and-day-out game of Spy vs. Spy, the exponentially growing number of pitches on which the game is being played might raise an eyebrow.

Posting a guard at the gate to check visitors' papers is a tried and true way of separating friend from foe. Figure 3a plots the number of appearances of "authentication" (upper/solid) and "credential" (lower/dashed) in the patent abstracts, while Figure 3b plots the number of appearances of "password" (upper/solid) and "biometric" (lower/dashed) in the patent abstracts.

Growth here is more linear than exponential of late, but the proliferation of new, useful, and non-obvious ideas is remarkable.

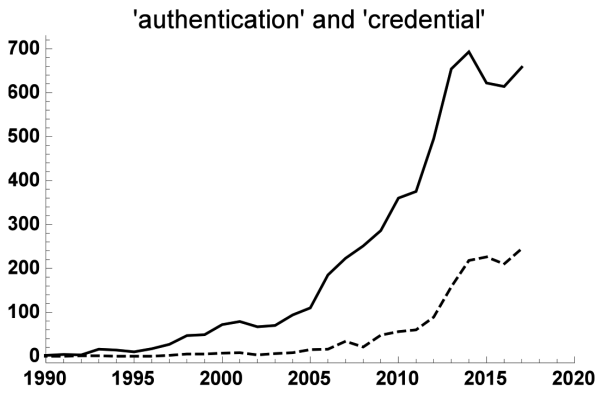

Figure 3a: Digital patents with "authentication" and "credential" in the patent abstract

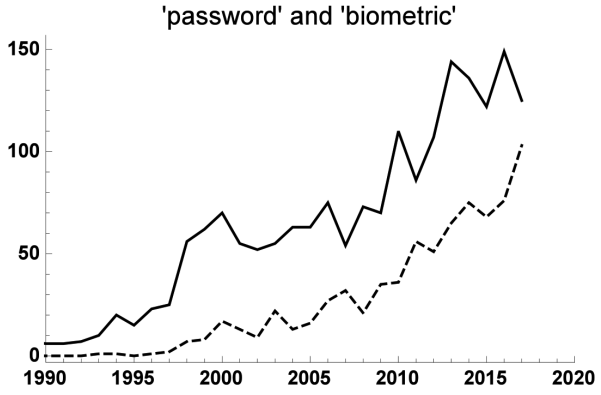

Figure 3b: Digital patents with "password" and "biometric" in the patent abstract

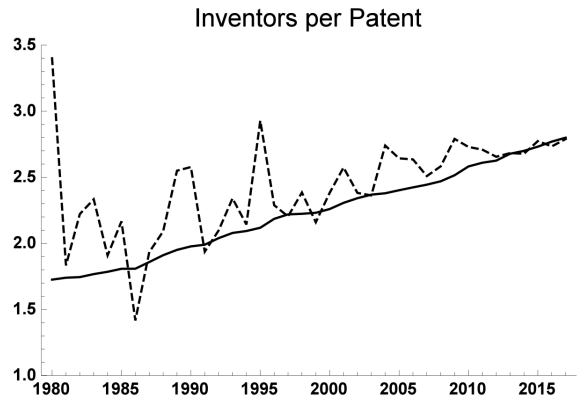

Figure 4: Inventors per patent: all patents (solid) and cybersecurity patents (dashed)

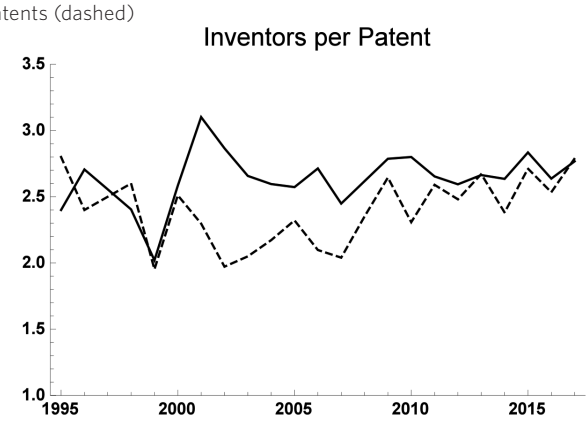

Figure 5: Inventors per patent: "authentication" (solid) and "biometric" (dashed)

Of course, that fact that the word "computer" appears in a patent abstract does not mean that the patent is about computers, and the same holds true for all of the other search terms discussed above. Nonetheless, one can safely conclude from this cursory analysis of the set of granted patents that inventive genius is ever harder at work on the cybersecurity problem.

Figure 4 shows the number of inventors per patent for all US patents and for cybersecurity patents. The fact that the number of inventors per patent has been growing slowly is well-known, and it comes as no surprise that whatever is driving this growth applies to cybersecurity patents *in toto* as well.

Curiously, if we restrict our attention to patents having to do with identity, the upward trend disappears. Figure 5 plots by year the average number of inventors for digital patents that have the word "authentication" (solid) or "biometric" (dashed) in their abstract. Roughly speaking, the average number of inventors per patent for patents having to do with identity is constant at about two and a half. Whatever it is driving the trend for most patents seems to be absent for this highly restricted subset.

The summary so far: where patent applications are coming from geographically has consolidated all but completely. Patents are probably the only strategy choice for cybersecurity inventors because users demand transparency in cybersecurity work much more than in other technical fields of endeavor. The subject-matter focus of cybersecurity patents may be moving toward defense (though it is possible that dual-use patents just avoid delineating their offensive capabilities). The fraction of all applications that are cybersecurity related is rising steeply, fueled by a growing fraction of all applications that are computer related and a growing fraction of computer-related applications that are for cybersecurity, growth compounded and compounded again. For any of these curves to radically change their course would surely mean something important.

We ask whether there really are this many new, useful, and non-obvious advances in cybersecurity. If there are, is this fast-rising tide of cybersecurity patents an unarguable confirmation of an equivalently fast-expanding digital attack surface? Or does the rising production of cybersecurity patents represent a correspondingly rising appreciation of the level of extant risk; that is to say, is society playing furious catch-up ball? Or is it something else again? Is it good or not good that while other sectors of the technological society require steadily larger and larger teams to come up with new, useful, and non-obvious ideas, in cybersecurity the teams are the same small size they have been for so long?