Defending Privacy ▪ The Dark Side of IoT ▪ Automating Cryptography

IEEE SECURITY & PRIVACY

March/April 2015
Vol. 13, No. 2

IEEE

IEEE computer society

ReliabilitySociety

Editors: Patrick McDaniel, mcdaniel@cse.psu.edu | Sean W. Smith, sws@cs.dartmouth.edu

Preprint. Published version appears in IEEE Security and Privacy, 13 (2): 94-98. March/April 2015.

Never Mind Pearl Harbor—What about a Cyber Love Canal?

Sean W. Smith | Dartmouth College
John S. Erickson | Rensselaer Polytechnic Institute

Pearl Harbor, as most US citizens were taught in school, was the site of a surprise Japanese attack on the US Navy, which catapulted the US into World War II. In the parlance of contemporary media, the term "Pearl Harbor" has come to denote the concepts of an infrastructure left completely undefended and how only a massive attack makes society take that exposure seriously.

As *IEEE Security & Privacy* readers know, our society's current information infrastructure is likely full of interfaces with exploitable holes. Pundits often discuss the potential of a "cyber Pearl Harbor"—sometimes in caution, referring to the devastation that could happen if an adversary systematically exploited the holes in exactly the wrong way, but sometimes in frustration that only such a large-scale disaster would create the social will to solve these security problems.

Yes, our current infrastructure's vulnerabilities are serious, attacks can have significantly negative consequences (as many executives at Sony have now learned), and both the computer security community and society at large need to keep working to improve things. However, focusing on malicious attacks on the current infrastructure might be distracting us from another looming challenge: the risk to emerging infrastructure due to carelessness.

A Dark Future

Many visionaries, researchers, and commercial actors herald the coming of the Internet of Things (IoT). Computers will no longer look like computers but rather like thermostats, household appliances, lightbulbs, clothing, and automobiles; these embedded systems will permeate our living environments and converse with each other and all other networked computers.

What's more, these systems will intimately interact with the physical world: with our homes, schools, businesses, and bodies—in fact, that's the point. In the visions put forth, the myriad embedded devices magically enhance our living environments, adjusting lights, temperature, music, medication, fuel flow, traffic lights, and elevators.

However, imagine a dark version of this world. Every object in the home—and every part of the home—is inhabited by essentially invisible computational boxes that can act on the physical environment. But rather than being helpful, these devices are evil, acting in bizarre, dangerous, or unexpected ways, either chaotically or coordinated in exactly the wrong way. We can't simply turn these devices off because no one knows where the off switches are. What's worse is that we don't even know where the devices are!

This vision of dark magic might inspire us to look to horror novels or science fiction for metaphors. However, real life has given us a better metaphor: environmental contamination. We've seen buildings contaminated by lead paint and asbestos and rendered uninhabitable by a chemical spill at a nearby dry cleaner, a research lab rendered uninhabitable by toxic mold, and superfund sites called "brownfields" that can't be built on. In all these cases, technology (usually chemical) intended to make life better somehow backfired and turned suburban utopias into wastelands.

What happened at the Pearl Harbor naval base is widely known. However, Americans over 50 might also remember Love Canal, a neighborhood of Niagara Falls, New York, that became synonymous with chemical contamination catastrophe. Vast amounts of chemical waste buried under land that later housed homes and schools led to massive health problems and the eventual evacuation and abandonment of these neighborhoods.

A cyber Pearl Harbor—a coordinated large-scale attack on our current computational infrastructure—would indeed be a bad thing. However, we should also be worried about a "cyber Love Canal"—buildings and neighborhoods, not to mention segments of our cyberinfrastructure, rendered uninhabitable by widespread "infection" and loss of control of the IoT embedded therein. The way we build and deploy devices won't work at the scale of the envisioned IoT and will backfire, like so many hidden chemical dumps. Continuing down this path will similarly lead to "cyber brownfields."

The Way We Build Things Now

Let's consider the way we build things now. A look at past and present IT shows that things don't work. To begin with, we keep getting input validation wrong. If programmers don't properly characterize valid input and ensure that programs check validity before acting, then adversaries can craft devious illegal inputs that trick machines into doing dangerous things. Buffer overflow, a classic example of this problem, was identified as a security problem before most current PhD students were born, yet exploits due to input validation flaws remain endemic.

We use overpowered components. Standard engineering practice says to reuse standard components rather than reinvent them each time. However, following this dictum can lead to security problems. For instance, we have seen a set-top box with limited internal storage had an OS (embedded Linux) that included support for remotely mounting malware, and a hospital's IT was brought down by a viral infection in a commodity OS buried in a radiology device.

In addition, we can't handle large-scale cryptographic infrastructure. Public-key cryptography is the best current technology to enable a diverse population of electronic identities to identify and authenticate. However, consider the population of "secure" webservers: only two million have proper X.509 certificates, and the supporting infrastructure still can't fully handle revocation or nontrivial trust paths.

We also can't handle human-oriented authentication. The de facto best current technology for authenticating humans—user IDs and passwords—doesn't work; humans share, reuse, and pick weak passwords,[1,2] and well-known default administrator passwords cause security holes. In the other direction, studies repeatedly show humans can't correctly interpret their machines' security signals.[3,4]

We can't effectively reason about exposure and risk. Consider the recent Shellshock vulnerability, an input validation bug in Bash that lay undiscovered for two decades. One of us (Smith) was concerned whether his Mac had Bash on its perimeter, reachable by an adversary. His machine wasn't a server, and he thought he'd locked down any unneeded services and ports—but even as a professional computer scientist, he couldn't say for sure. (It turns out that his machine did expose Bash, apparently as part of the Dynamic Host Configuration Protocol handshake.)

"Things don't work" is the security idealist's standard rant. A more honest observation is that, although flawed, things work well enough to keep it all going. For the most part, we know where the machines are—workstations and laptops in offices, servers in datacenters. OSs and software are new enough to still be updated, and machines are usually expensive enough to justify users' attention to maintenance and patching before too many compromises happen.

Machines don't last for decades. We know when we're working with them. The average user doesn't need secure connections to that many machines—perhaps some Web servers and a mail server. A few million certificates, a few dozen trust roots, and trust paths of length one might suffice; revocation might be rare enough that manual mechanisms suffice. The IT infrastructure is compromisable and compromised, with occasional lost productivity and higher fraud losses amortized over a large population, yet life goes on, mostly. The fact that we're writing this article on networked machines while the Web continues to work proves that.

If We Keep Doing That

However, in the IoT, the numbers, distribution, embeddedness, and invisibility of devices will change the game. Suppose we build the IoT the same way we built the current Internet. When the inevitable input validation bug is discovered, there will be orders of magnitude more vulnerable machines. Will embedded machines be patchable? Will anyone think to maintain inexpensive parts of the physical infrastructure? Will machines and software last longer than the IoT startups that create them? Will anyone even remember where the machines are? January 2015 brought news that a few recent well-publicized distributed denial-of-service attacks were apparently advertisements for a botnet housed on home wireless routers—overlooked machines that don't look like machines.[5] Imagine a world in which everyone needed to update each door, each electrical outlet, and perhaps even each lightbulb on Patch Tuesday.

When the inevitable happens, what will a compromised machine in the IoT be able to do? It's no longer just housing data; it's controlling boiler temperatures, elevator movement, automobile speed, fish tank filters, and insulin pumps. Consider the effects of denial-of-service on our physical infrastructure. Recently, it was –15°F in New Hampshire. How many burst pipes and damaged buildings would we have had if a virus shut down all the heating systems? The recent book *Five Days at Memorial* chronicled the horrors of being trapped in a New Orleans hospital when Hurricane Katrina shut down basic infrastructure, including electricity, transport, communication.[6] Can an infection in the IoT cause similar infrastructure loss?

Fail-stop is bad enough, but compromised machines in the IoT can do more than simply stop; they can behave arbitrarily. What havoc might happen when elevators, automobiles, and door locks start behaving arbitrarily? A decade ago, a compromise at one of our universities (Dartmouth College) led to a large server being co-opted to distribute illegal content—annoying, but relatively harmless. What will happen when schools, homes, apartment buildings, and shopping malls are full of invisible, forgotten, and compromised smart devices?

If a computer professional has trouble reasoning about which computers (that look like computers) in the house might expose the Bash vulnerability today, how will anyone reason effectively about risk and exposure when thousands of times more computers are in the house and they no longer look like computers? Furthermore, if we keep using standard commodity operating systems and tools, machines that look like X might in fact act very differently (just as set-top boxes can act as man-in-the-middle nodes on LANs), further complicating reasoning about what's doing what.

It's also unclear how cryptographic infrastructure will scale to the IoT (as we considered for the smart grid in "Cryptographic Scalability Challenges in the Smart Grid"[7]). There's one Amazon (albeit probably with many datacenters). The overhead of setting it up can justify a bit of cost in getting Web trust roots to sign off on the public keys. But in the IoT, we will have many orders of magnitude more devices, far more mobile and with far less overhead. Yet, if they act autonomously, they need to be identified and authenticated. Can a toaster or lightbulb generate strong cryptographic keys? (Researchers have already observed systematic flaws in how current embedded systems do this.[8]) Who will issue an X.509 certificate to a toaster or a lightbulb? Who will be in a position to know it's a lightbulb in that corner of my living room? Will central trust roots or remote servers need to have deeply personal data, will customers operate their own trust roots, or will we overlay an identity public key infrastructure with an attribute PKI? With these numbers of devices, how big will certificate revocation lists get? With a multiplicity of trust roots, how long will trust paths get?

Beyond the cryptographic infrastructure, cryptography itself is a challenge of the cryptography. How long will lamps, electrical outlets, and washing machines last—and will the cryptography last as long? For instance, the appliances in at least one of the author's houses are more than 20 years old. Would you trust now the cryptography deemed "reasonably secure" 20 years ago? When asked, one colleague said "there's RSA," but what about the recommended modulus length and the associated hash and padding algorithms? Remember the quick deaths of MD5 and ISO9796?

Bleak Truths We Must Avoid

The IoT will continue to grow exponentially and evolve in remarkable ways. As it does, we must acknowledge that we need to prepare for and, where possible, take actions to avoid certain "fundamental truths."

First, although some vendors will try to push top-down ecosystems, the IoT will probably grow organically, a global mashup of heterogeneous components with no top-down set of principles determining its emergent behavior. This lack of control might help segment security problems at a macro scale but will be a disturbing reality for any entity that would prefer to centrally control the IoT as a large, intelligent, interconnected network. In particular, we should expect abandoned or otherwise legacy segments of today's IoT to have unanticipated interactions with and impact on the Internet of tomorrow, like buried drums of highly toxic cyberwaste.

The creators of the IoT are only human and tend to replicate components at every opportunity. Industry segments are rooted in system designers' tendency to apply their favorite tools across the problem space. Common hardware and firmware libraries will show up on the IoT in surprising places; we can expect to see smart snowboards, thermostats, lightbulbs, and scientific instruments using the same connected microcontrollers and firmware. This hidden homogeneity can be bad, because just about anything having a particular "genetic" vulnerability might be compromised. However, a systematic homogeneity might also be beneficial if well-designed and inherently safe subsystems—those having the right "IoT DNA"—are widely adopted.

Consumers care little about testing regimes, product recalls, and other measures enacted in their best interest. IoT watchdog groups might start testing for compliance against a set of IoT safety standards, and governments might impose IoT safety regulations and dictate recalls, but we can expect consumers to purchase and deploy substandard devices. The IoT industry could introduce safety-assuring protocols—for instance, applying block chains for IoT messaging.[9] However, providers and customers will surely look elsewhere if such measures raise costs without adding significant and obvious value.

Finally, consumers' hunger for the latest and greatest might save their IoT, but enterprises' conservatism could break theirs. We might be able to exploit consumers' inherent desire for newer, better, faster to promote the ecosystem's health, at least among the consumer-facing IoT segments. We can expect today's IoT to get old fast, even without producers intentionally designing them to go obsolete quickly. Bad actors might get adopted quickly, but they might also fade away quickly.

IoT in the enterprise might prove to be a counterexample to this notion that "churn" will keep the IoT healthy, as it's always reluctant to avoid the expense of upgrading already deployed systems. Left unperturbed, the commercial/industrial IoT sector might prove to be the Windows XP of the IoT, full of homogeneous badness that won't go away and persisting through an unwillingness to embrace improved, potentially safer systems.

What Do We Do?

It's tempting to repeat the old joke about the patient telling the doctor "it hurts when I do this," to which the doctor replies "then don't do that." History shows that we keep building and deploying IT systems that inadvertently contain serious vulnerabilities, which we later try to patch before too much damage is done. If the IoT's scale and distribution make this "solution" impractical, then maybe we can just start building systems without the vulnerabilities! Unfortunately, it's not at all realistic to assume that, starting today, we'll suddenly start doing things much better. We need some game changers: maybe a new programming language, a new approach to highly reliable input validation (e.g. Sassaman et al),[10] or a way to use massively parallel multicore cloud computing to thoroughly fuzz-test and formally verify.

Another approach might be a new way to structure systems to mitigate damage when they're compromised. Instead of a smart grid, perhaps we need a "dumb grid": well-tested commodity operating systems, compilers, languages, and such that are modular, so developers can break off unneeded pieces. Or maybe we can use the extra cores from Moore's Law to make each IoT system multicultural: N distinct OSs and implementations, which aren't likely to be vulnerable in the same way at the same time.

Biology tells us that one of the problems with cancer is when the telomeres mechanism, which limits the number of times a cell can divide, stops working, allowing cell growth to run reckless. Maybe we can mitigate the problem of unpatched and forgotten IoT systems by building in a similar aging mechanism: after enough time (or enough time without patching), they automatically stop working. Of course, this can be dangerous as well. Perhaps instead, for each kind of IoT node, we can define a safe, inert "dumb" state to which they revert after a time.

These are just a few ideas. If we want the IoT to give us a safe and healthy future, we have our work cut out for us. ■

References

1. D. Florencio and C. Herley, "A Large-Scale Study of Web Password Habits," *Proc. World Wide Web Conf.*, 2007, pp. 657–666.
2. S. Gaw and E. Felten, "Password Management Strategies for Online Accounts," *Symp. Usable Privacy and Security* (SOUPS 06), 2006, pp. 44–55.
3. R. Dhamija, M. Hearst, and J.D. Tygar, "Why Phishing Works," *Proc. SIGCHI Conf. Human Factors in Computing Systems*, 2006, pp. 581–590.
4. S. Schechter et al., "The Emperor's New Security Indicators," *IEEE Symp. Security and Privacy*, 2007, pp. 51–65.
5. B. Krebs, "Lizard Stresser Runs on Hacked Home Routers," KrebsOnSecurity, Jan. 2015; http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers.
6. S. Fink, *Five Days at Memorial: Life and Death in a Storm-Ravaged Hospital*, Deckle Edge, 2013.
7. S.W. Smith, "Cryptographic Scalability Challenges in the Smart Grid," *Innovative Smart Grid Technologies*, 2012; www.cs.dartmouth.edu/~sws/pubs/gridpki.pdf.
8. N. Heninger et al., "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices," *Proc. 21st USENIX Security Symp.*, 2012, p. 35.
9. P. Brody and V. Pureswaran, *Device Democracy: Saving the Future of the Internet of Things*, IBM Global Business Services Executive Report, 2014.
10. L. Sassaman, et al., "Security Applications of Formal Language Theory," *IEEE Systems J.*, vol. 7, no. 3, 2013, pp. 489–500.

Sean W. Smith is a professor of computer science and research director of the Institute for Security, Technology and Society at Dartmouth College. Contact him at sws@cs.dartmouth.edu.

John S. Erickson is the director of operations at the Rensselaer Institute for Data Exploration and Application (IDEA) at Rensselaer Polytechnic Institute. Contact him at erickj4@rpi.edu.