Understanding Resilience of Large-Scale and Long-Lived EDS

Invisible and Forgotten: Zero-Day Blooms in Smart Grid and the IoT

Emily Holt, Kartik Palani, Sergey Bratus, David Nicol, and Sean Smith

GOALS

In energy delivery infrastructure and elsewhere, we're seeing computational infrastructure transform into networks of devices distributed massively on almost any axis imaginable. Humans cannot effectively reason about security when devices become too long-lived, too cheap, too invisible, and too numerous.

- What are the implications of vulnerability discoveries and mitigation strategies in this emerging infrastructure?
- What is the aggregate impact of the proposed solutions? How many of which kind would help the most?

Smartness everywhere disrupts the penetrate-and-patch paradigm!

FUNDAMENTAL QUESTIONS/CHALLENGES

In the current state of the art and practice, embedded systems are rife with security holes, with zero-days and forever-days. The smart grid and IoT will have even more—and be even more intimately tied to physical infrastructure.

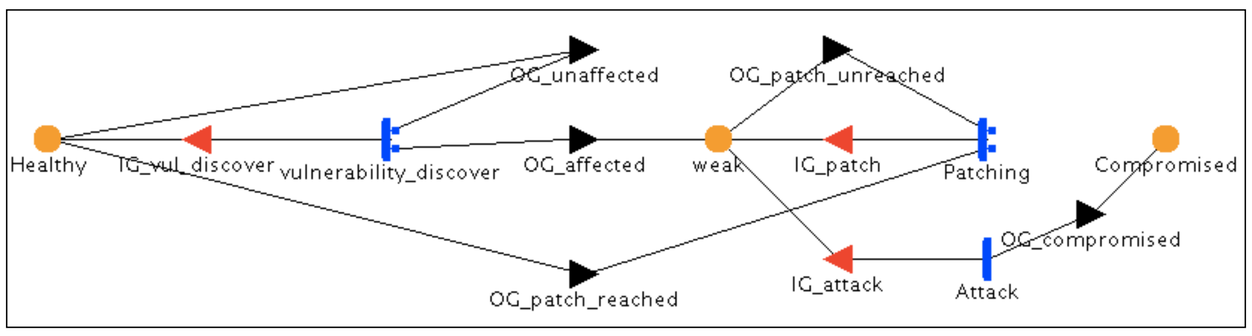
- Will updates to security problems become more difficult to implement as devices become increasingly invisible?
- Will unmatched software persist longer in smart grid and IoT devices? What if the devices themselves outlive their vendors?
- Will smart grid and IoT devices be more difficult to patch because of network connectivity/reachability issues?
- Will security contributions of anti-virus solutions decrease because of devices' inability to run them?
- Will the physical structure and connectivity of devices increase the damage of successful attacks?
- Will the increased size of the device population reduce the effectiveness of the penetrate-and-patch paradigm?
- How can we avoid the spread of malicious attacks in a less effective paradigm as the legacy of previous malicious attacks—such as the holes enabling Stuxnet—still persist today?

https://threatpost.com/researcher-finds-csrf-bug-in-wind-turbine-software/113198/
https://threatpost.com/plaintext-credentials-threaten-rle-wind-turbine-hmi/113354
https://securityledger.com/2015/06/x-rays-behaving-badly-devices-give-malware-foothold-on-hospital-networks/
https://threatpost.com/pair-of-bugs-open-honeywell-home-controllers-up-to-easy-hacks/113965

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
http://www.bbc.com/news/technology-30575104
http://blog.trendmicro.com/trendlabs-security-intelligence/is-anonymous-attacking-internet-exposed-gas-pump-monitoring-systems-in-the-us/
https://news.vice.com/article/windows-31-is-still-alive-and-it-just-killed-a-french-airport

RESEARCH PLAN

- Quantify the relative differences in security conditions from IoC to IoT.
- Predict the growth rate of zero-days in unpatched software using models that use historical patterns to predict future trends in vulnerability reporting.
- Determine causes of blooms in vulnerability reporting using past data in order to make predictions for the future.
- Use simulations to quantify future risk and possible success rates of various preventative measures for attacks on IoT software using the model pictured below:

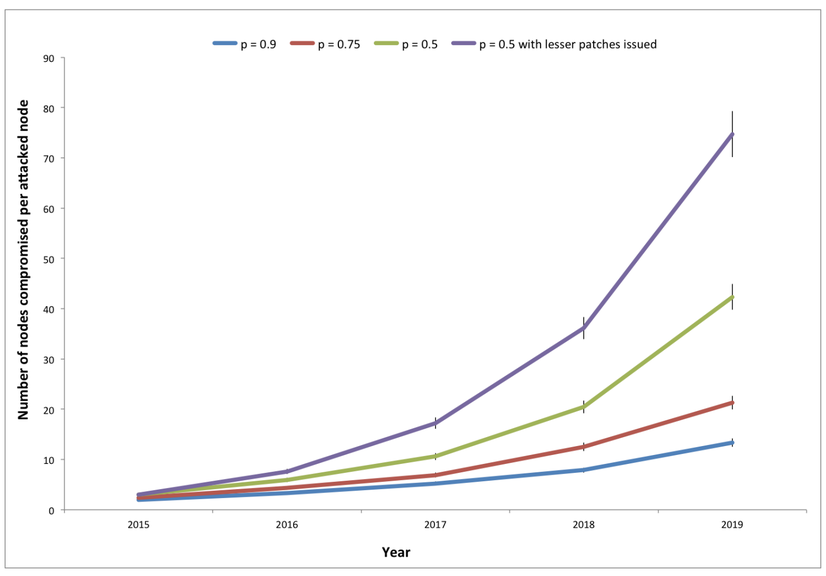


INITIAL REPORT

K. Palani, E. Holt, and S. Smith. "Invisible and Forgotten: Zero-Day Blooms in the IoT." *The 1st IEEE PerCom Workshop on Security, Privacy, and Trust in the IoT.* March 2016. http://www.cs.dartmouth.edu/~sws/pubs/phs16.pdf

RESEARCH RESULTS

- When a patch is issued for every vulnerability that is discovered, there are still multiple nodes that get affected when a single node is attacked, even when 90% of the patches reach the nodes.
- As patchability becomes worse, as can be seen for the cases where p = 0:75 and p = 0:5, more nodes get affected by a single failed node.
- That shows the high amount of dependence in the IoT mesh network scenario.
- When we retard the patchability and also consider that only 90% of the vulnerabilities have patches issued/discovered, for every device that is attacked, more than 80 devices will be potentially compromised.
- The probability that a patch will successfully reach every device is going to decline drastically.
- As patchability gets worse, the highly interconnected and dependent nature of the IoT would mean that a single exploitation of a vulnerability on a single node would lead to potential compromise of various other nodes.



The number of nodes that get compromised per attacked node over time for different patchability constants (p), which is the probability that a patch successfully reaches a node.

BROADER IMPACT

- Long-term goal is not to forecast doom but rather to avoid it. To that end, a model to analyze vulnerability impact in the IoT will also extend to evaluating the efficacy and performance impact of various proposed mitigation techniques.
- By using our model to study other communication architectures for IoT that have different levels of interdependence, we will gain a better understanding of the schemes that need to be implemented in order to avoid spreads of attacks.

INTERACTION WITH OTHER PROJECTS

- This work motivates the urgent need for the scalable and fast authentication techniques being proposed in the Namespace and Cryptographic Complexity work by Palani (UIUC), Nicol (UIUC), Anantharaman (Dartmouth) and Smith (Dartmouth).
- The work also draws parallels from previous work by Nicol (UIUC) studying worm infestations in the large-scale Internet.
- This work also relates to the LangSec work of Bratus (Dartmouth) exploring scientific approaches to stopping input validation vulnerabilities.

FUTURE EFFORTS

- Extend the model to look at more sophisticated topologies and more sophisticated threat models.
- Revise the model to reflect the security implications of the various topological choices—and of having a superposition of several of them.
- Take into consideration heterogeneous vulnerability/patching patterns and lags, topological implications on patching and attacks, emergence of thingbots, and net physical impact of attacks and thingbots.

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY