Featured news

- IoT: Security misconceptions, expectations, and the future
- Aggressive tactics from DD4BC extortionist group revealed
- Global cyber insurance market to grow to over $20 billion by 2025
- Cyberespionage group exploits satellites for ultimate anonymity
- 2015 saw 888 data breaches, 246 million records compromised worldwide
- Security pros acknowledge risks from untrusted certificates but take no action
- New Android malware could inflict $250,000 of losses
- Microsoft pushes out security updates, plugs holes actively exploited by attackers
- The White House sprints to lock down data
- Half of iPhones on corporate networks run outdated iOS versions
- 0-day bugs in Kaspersky and FireEye products found, exploits disclosed
- Carbanak APT still targeting high-value financial institutions and casinos
- How talking to recognition technologies will change us
- Android ransomware masquerades as Adult Player app, takes photo of victim
- Vulnerabilities in WhatsApp Web affect 200 million users globally
- Ashley Madison developers not big on security

Internet of Things: Security misconceptions, expectations, and the future

by Mirko Zorz - Editor in Chief - Thursday, 10 September 2015.

Nitesh Dhanjani is a well-known security researcher, writer, and speaker. He is currently Executive Director, Cybersecurity, at Ernst & Young, where he advises C-suite executives at the largest Fortune 100 corporations on how to establish and execute complex multimillion-dollar cybersecurity programs.

He recently released his latest book, Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts, so it was the perfect time to have a conversation about IoT security.

What are the most significant misconceptions people have when it comes to IoT security, even in the information security community?

We are biologically wired to concede to optimism bias - the mistaken belief that the one's chances of experiencing a negative event are lower than that of other people. When it comes to the risk posed by attacks against IoT devices, this perception is further fueled by the notion that living in a traditional world of disconnected devices will continue to be an option.

We have already seen demonstrations of attacks, such as those against connected cars and medical devices, that can result in physical harm or the loss of life. As our society becomes increasingly reliant on devices around us to be connected, the line between our virtual and physical spaces will blur. Once vulnerabilities in popular IoT devices begin to be actively exploited to cause harm, our default biases attuned to favor optimism will shatter.

Within the information security community, I find that there is lack of appreciation for the profound responsibility we have to help secure devices that human-kind is going to rely upon to survive and even migrate to other planets. We dwell upon the criticality of state sponsored attackers with a myopic comprehension of the risk that awaits us. I feel we must begin to look upon connected systems such as smart cities, our increased reliance on medical devices that are online, and our projects to preserve our species to survive beyond planet Earth (such as what Elon Musk is doing with SpaceX).

We also need to start thinking through how best we ought to have conversations around existential threats such as super-intelligence. My intention as been to help us approach the topic of IoT security by taking a look at security contained within devices that we are already relying upon today. It is though this tangible understanding of the current landscape that we can being to build a strategy that will see us to a sustainable future.

How do you expect information security to evolve with billions of new devices getting online in the next few years?

We are going to see situations that will enable various types of threat agents with the ability to cause physical harm towards select targets as well as a sizable groups of populations. This is also likely to include violations of privacy orchestrated by exploiting the ecosystem of devices that we are going to come to depend upon. Threat agents beyond nation states, i.e. terrorist gangs, cyber-bullies, and predators are going to exploit connected devices to orchestrate scenarios that go well beyond traditional intentions of stealing mere financial information.

1 | 2 | Next page

books Internet of Things tips

Spotlight

1 2 3 4 5

2015 saw 888 data breaches, 246 million records compromised worldwide

What we're continuing to see is a large ROI for hackers with sophisticated attacks that expose massive amounts data records. Cyber criminals are still getting away with big and very valuable data sets.

Weekly newsletter

Reading our newsletter every Monday will keep you up-to-date with security news.

Email @ Address

Daily digest

Receive a daily digest of the latest security news.

Email @ Address

MISS the future compromised ultimate anonymity change us

Thu, Sep 10th

Back to TOP