# Cyber-insecurity: PL to the Rescue

Michael Hicks
University of Maryland

# Security breaches

Just a few:

- **TJX** (2007) - 94 million records*
- **Adobe** (2013) - 150 million records, 38 million users
- **eBay** (2014) - 145 million records
- **Anthem** (2014) - Records of 80 million customers
- **Target** (2013) - 110 million records
- **Heartland** (2008) - 160 million records

**containing SSNs, credit card nums, other private info*

https://www.oneid.com/7-biggest-security-breaches-of-the-past-decade-2/

# Defects and Vulnerabilities

- Many (if not all of) these breaches begin by exploiting a **vulnerability**

- This is a *security-relevant* **software defect** (bug) or **design flaw** that can be **exploited** to effect an undesired behavior

- The **use of software is growing**
  - So: more bugs and flaws
  - Especially in places that are new to using software

Google
2B LOC

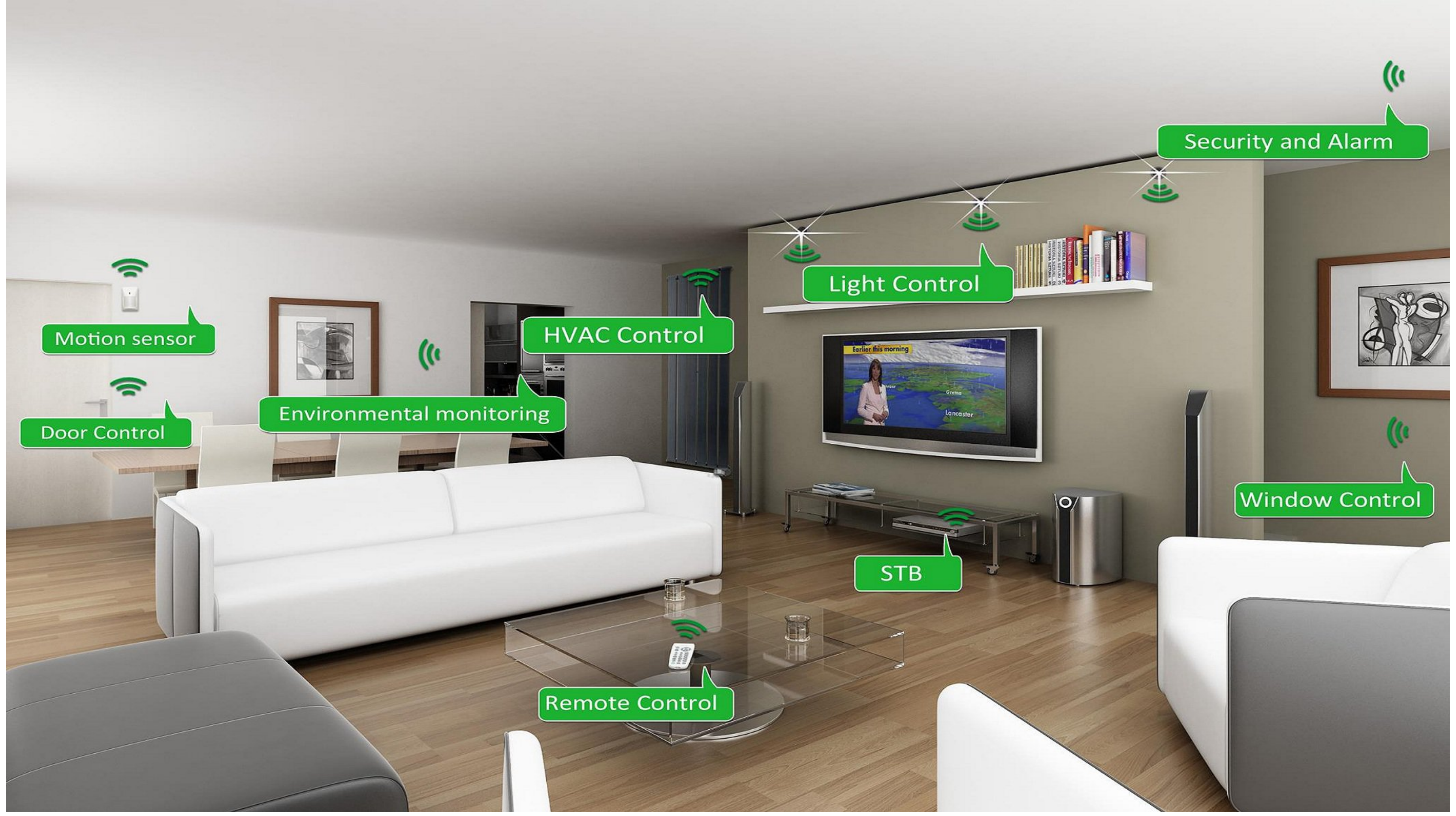
Windows
50M LOC

…

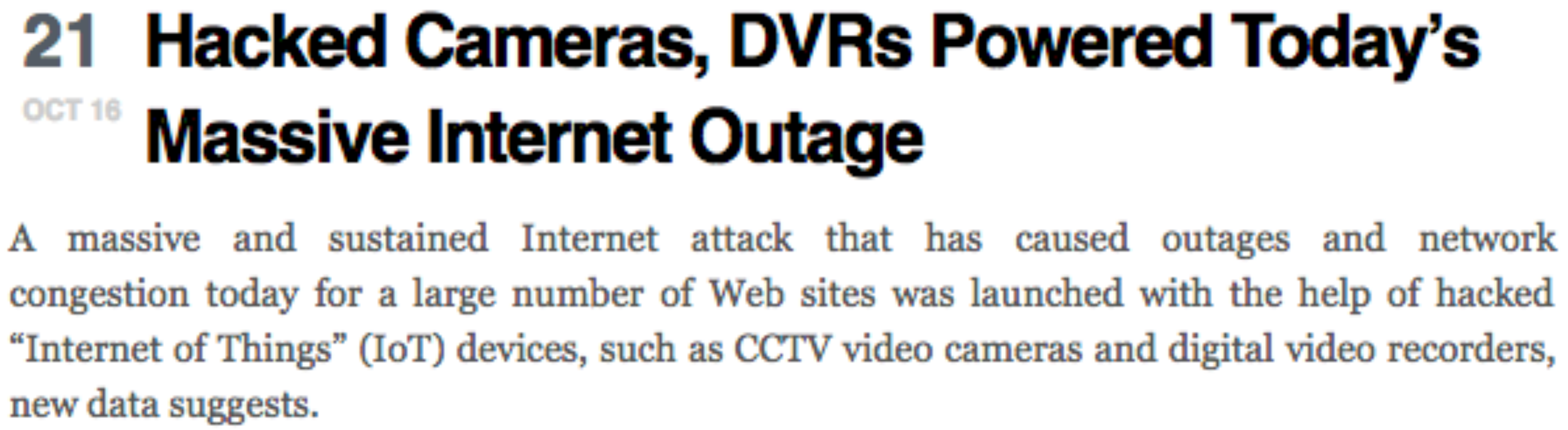
…

# “Internet of Things” (IOT)

Amazon Alexa

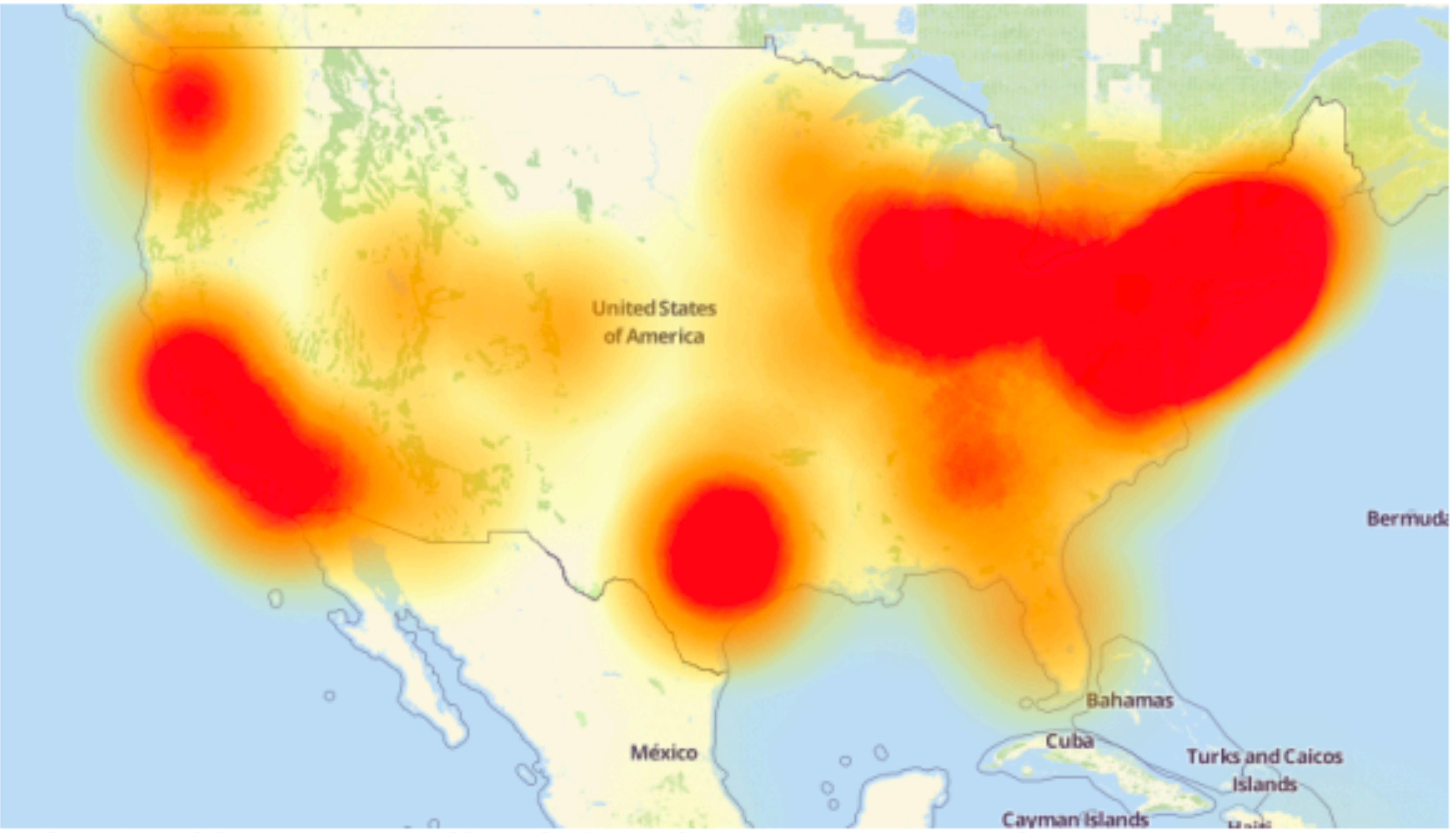


Google Home



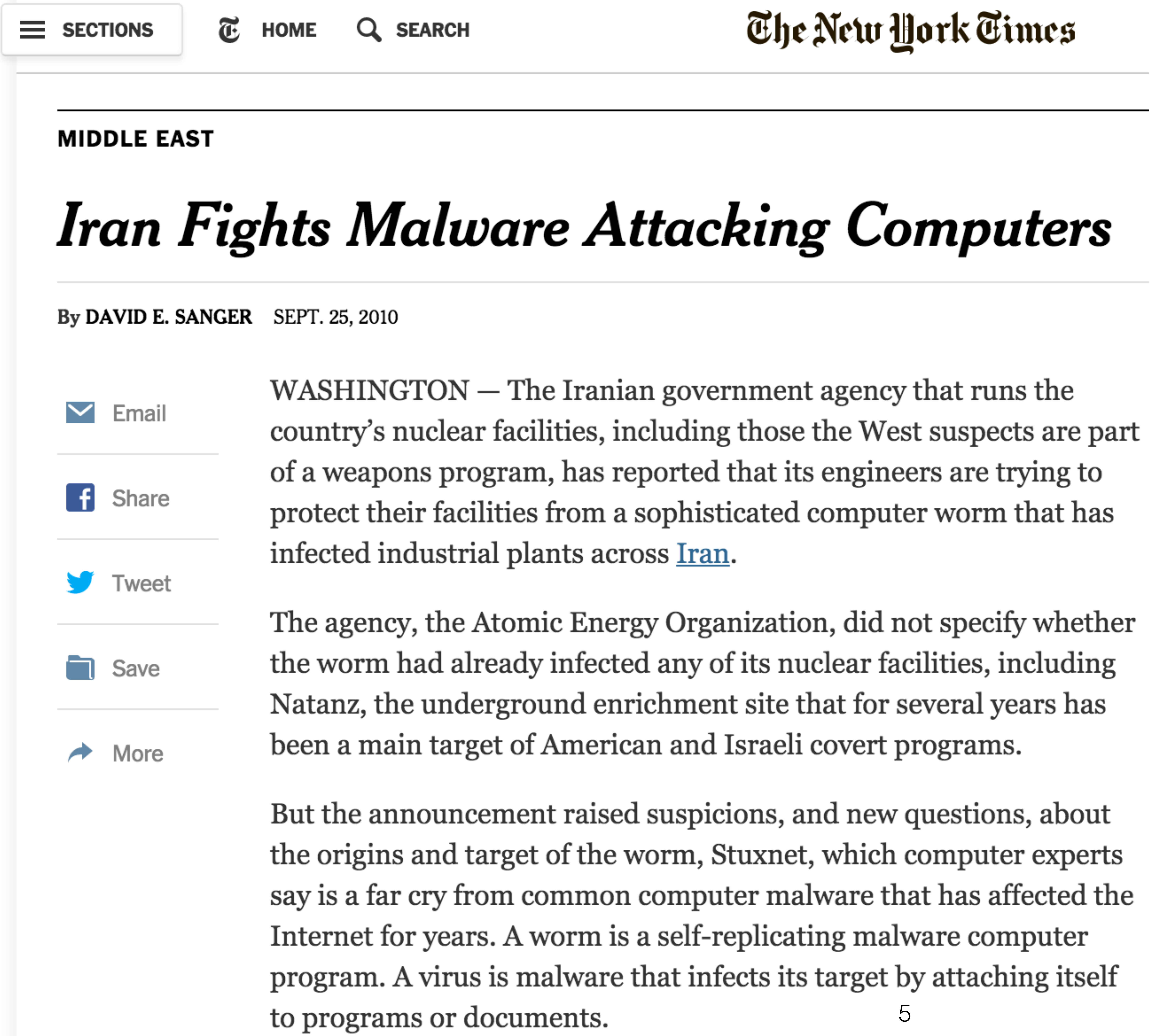
21 OCT 16 **Hacked Cameras, DVRs Powered Today’s Massive Internet Outage**

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked “Internet of Things” (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.



*A depiction of the outages caused by today’s attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.*

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/



MIDDLE EAST

# *Iran Fights Malware Attacking Computers*

By DAVID E. SANGER SEPT. 25, 2010

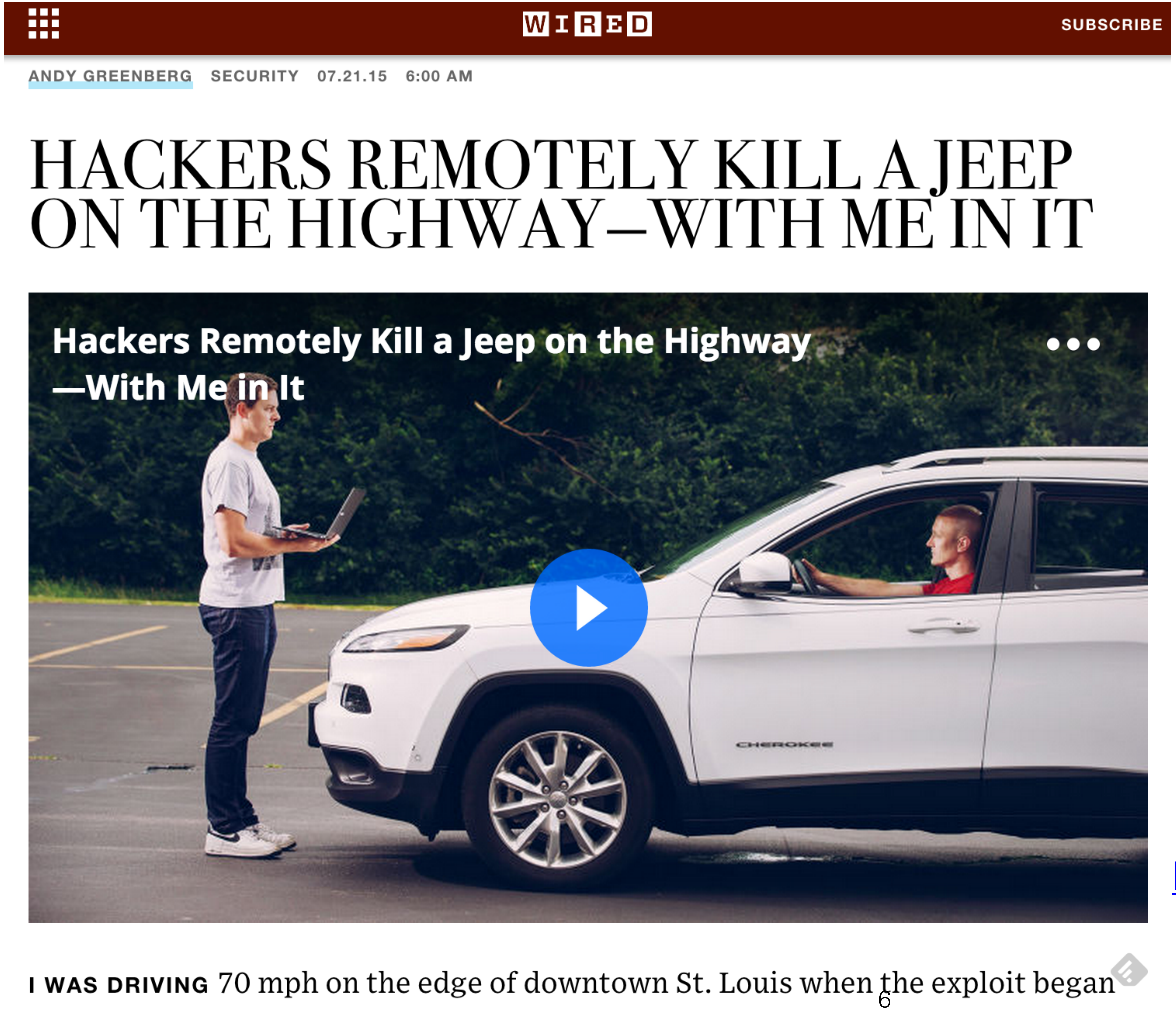
WASHINGTON — The Iranian government agency that runs the country’s nuclear facilities, including those the West suspects are part of a weapons program, has reported that its engineers are trying to protect their facilities from a sophisticated computer worm that has infected industrial plants across Iran.

The agency, the Atomic Energy Organization, did not specify whether the worm had already infected any of its nuclear facilities, including Natanz, the underground enrichment site that for several years has been a main target of American and Israeli covert programs.

But the announcement raised suspicions, and new questions, about the origins and target of the worm, Stuxnet, which computer experts say is a far cry from common computer malware that has affected the Internet for years. A worm is a self-replicating malware computer program. A virus is malware that infects its target by attaching itself to programs or documents.

Stuxnet specifically targets … processes such as those used to control … **centrifuges for separating nuclear material**. Exploiting four zero-day flaws, **Stuxnet** functions by targeting machines using the Microsoft Windows operating system …, then seeking out Siemens Step7 software.

http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html



WIRED SUBSCRIBE

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

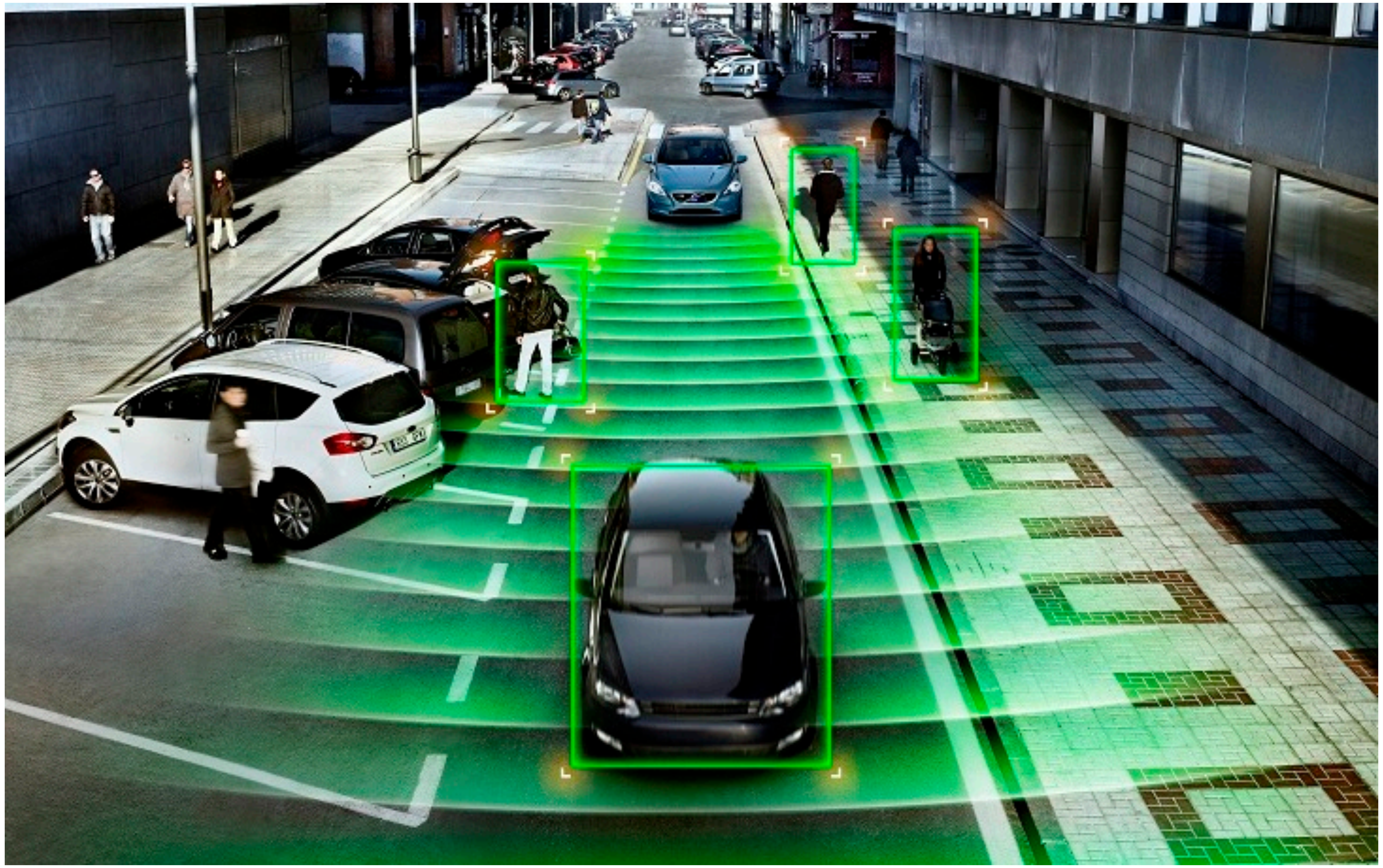
# HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

**I WAS DRIVING** 70 mph on the edge of downtown St. Louis when the exploit began

The result of their work was a hacking technique—what the security industry calls a zero-day exploit—that can **target Jeep Cherokees and give the attacker wireless control**, via the Internet, to any of thousands of vehicles.

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

# Driverless Cars



# Considering **Correctness**

- **All software is buggy**, isn’t it? Haven’t we been dealing with this for a long time?
- A **normal user never sees most bugs**, or figures out how to **work around** them
- Therefore, **companies fix the most likely bugs**, to save money

# Considering **Security**

Key difference:

***An attacker is not a normal user!***

- The attacker **will actively attempt to find defects**, using unusual interactions and features
  - A typical interaction with a bug results in a **crash**
  - An attacker will work to **exploit** the bug to do **much worse**, to achieve his goals

# Cyber-defense?

# Cyber-defense?

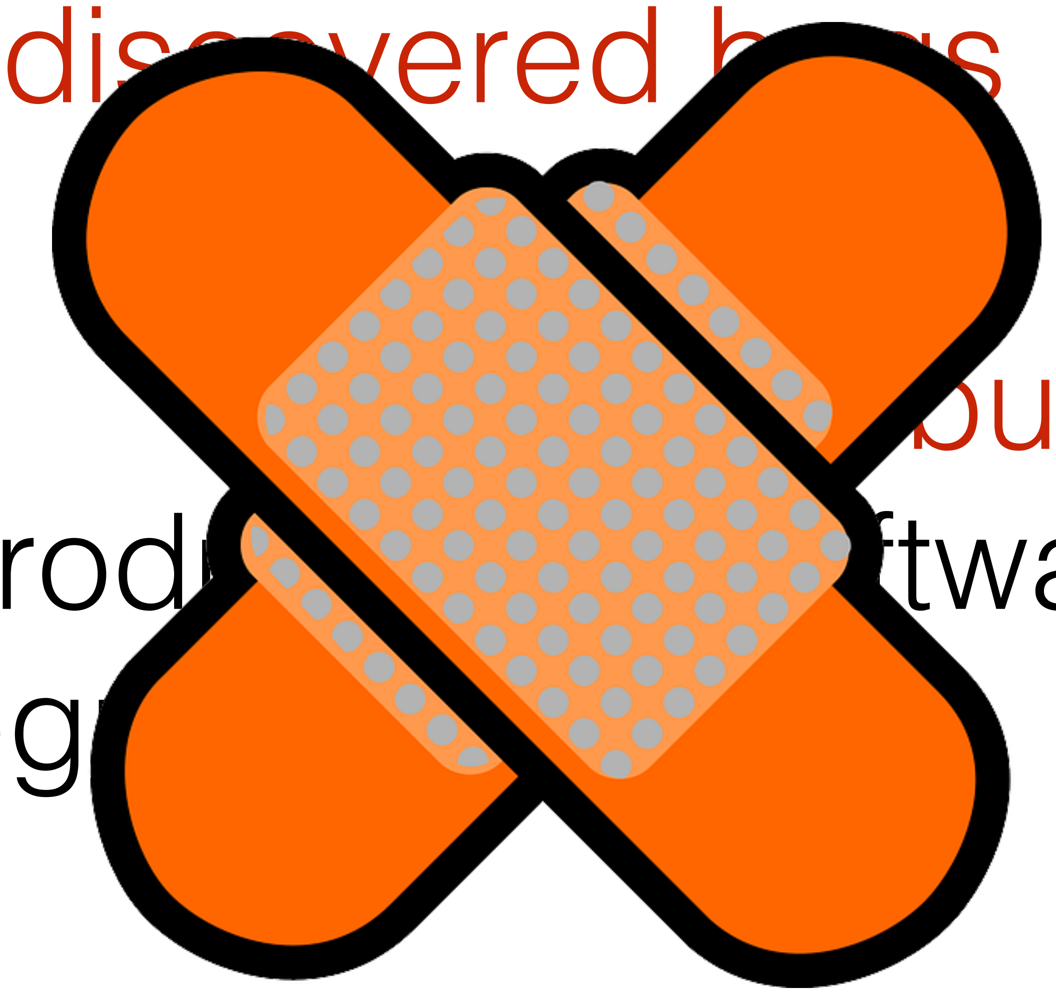
Popular technologies such as **firewalls**, **anti-virus**, and **intrusion detection/prevention**, attempt to detect the attacks themselves.

But **new attacks** can be produced that avoid detection but **exploit the same vulnerabilities**

# Penetrate and Patch

1. Find a vulnerability
2. Develop patch
3. Deploy patch (and detection signature)

*But*: Still vulnerable to undis vered b s

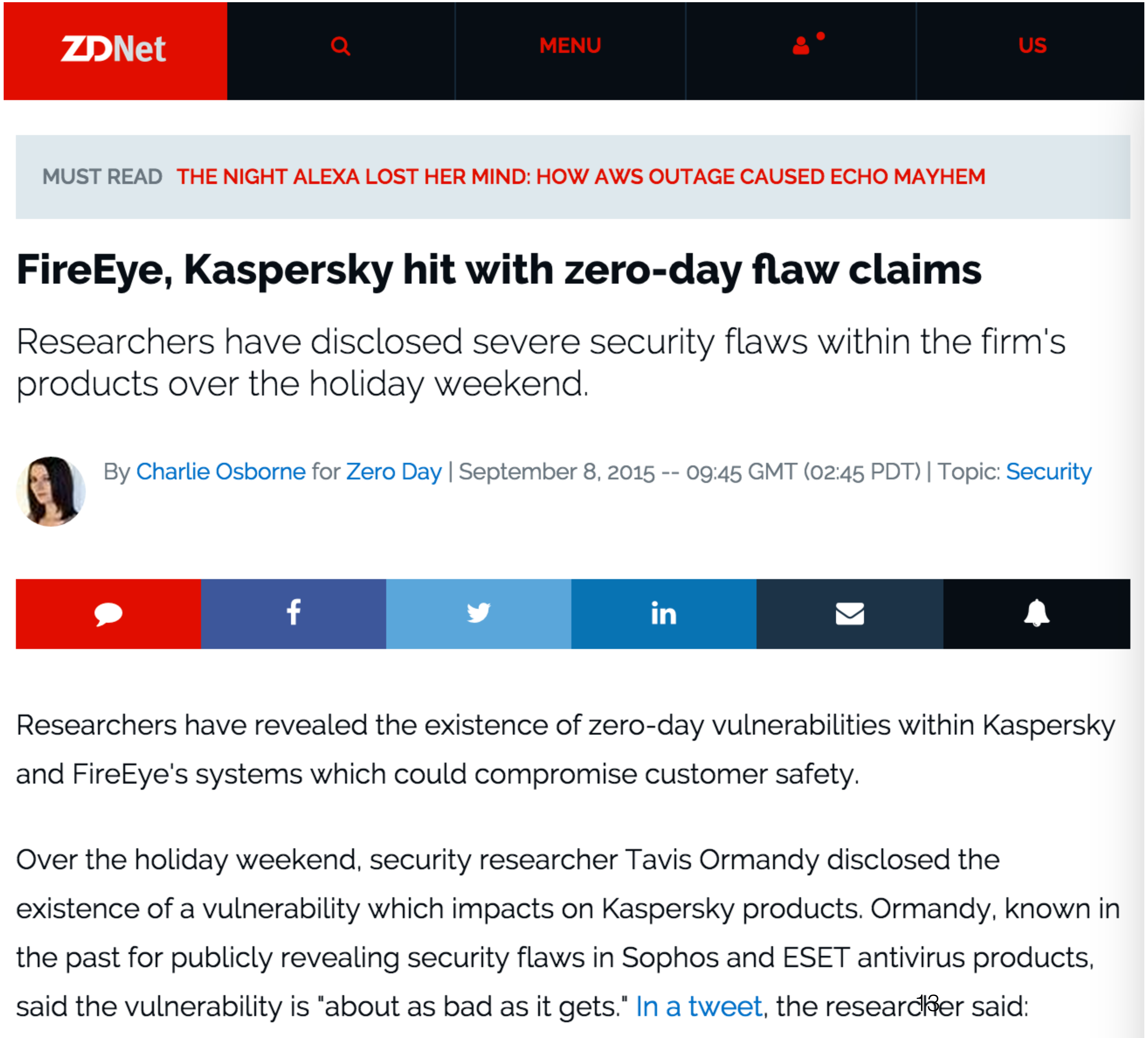


bugs

introd ftware

upg

# and **bugs in security products** themselves!



MUST READ THE NIGHT ALEXA LOST HER MIND: HOW AWS OUTAGE CAUSED ECHO MAYHEM

**FireEye, Kaspersky hit with zero-day flaw claims**

Researchers have disclosed severe security flaws within the firm's products over the holiday weekend.

By Charlie Osborne for Zero Day | September 8, 2015 -- 09:45 GMT (02:45 PDT) | Topic: Security

Researchers have revealed the existence of zero-day vulnerabilities within Kaspersky and FireEye's systems which could compromise customer safety.

Over the holiday weekend, security researcher Tavis Ormandy disclosed the existence of a vulnerability which impacts on Kaspersky products. Ormandy, known in the past for publicly revealing security flaws in Sophos and ESET antivirus products, said the vulnerability is "about as bad as it gets." In a tweet, the researcher said:

Security researcher Tavis Ormandy disclosed the existence of **a vulnerability which impacts on Kaspersky [security] products**.

Hermansen, [another researcher,] publicly disclosed a zero-day **vulnerability within cyberforensics firm FireEye's security product**, complete with proof-of-concept code.

http://www.zdnet.com/article/fireeye-kaspersky-hit-with-zero-day-flaw-claims/

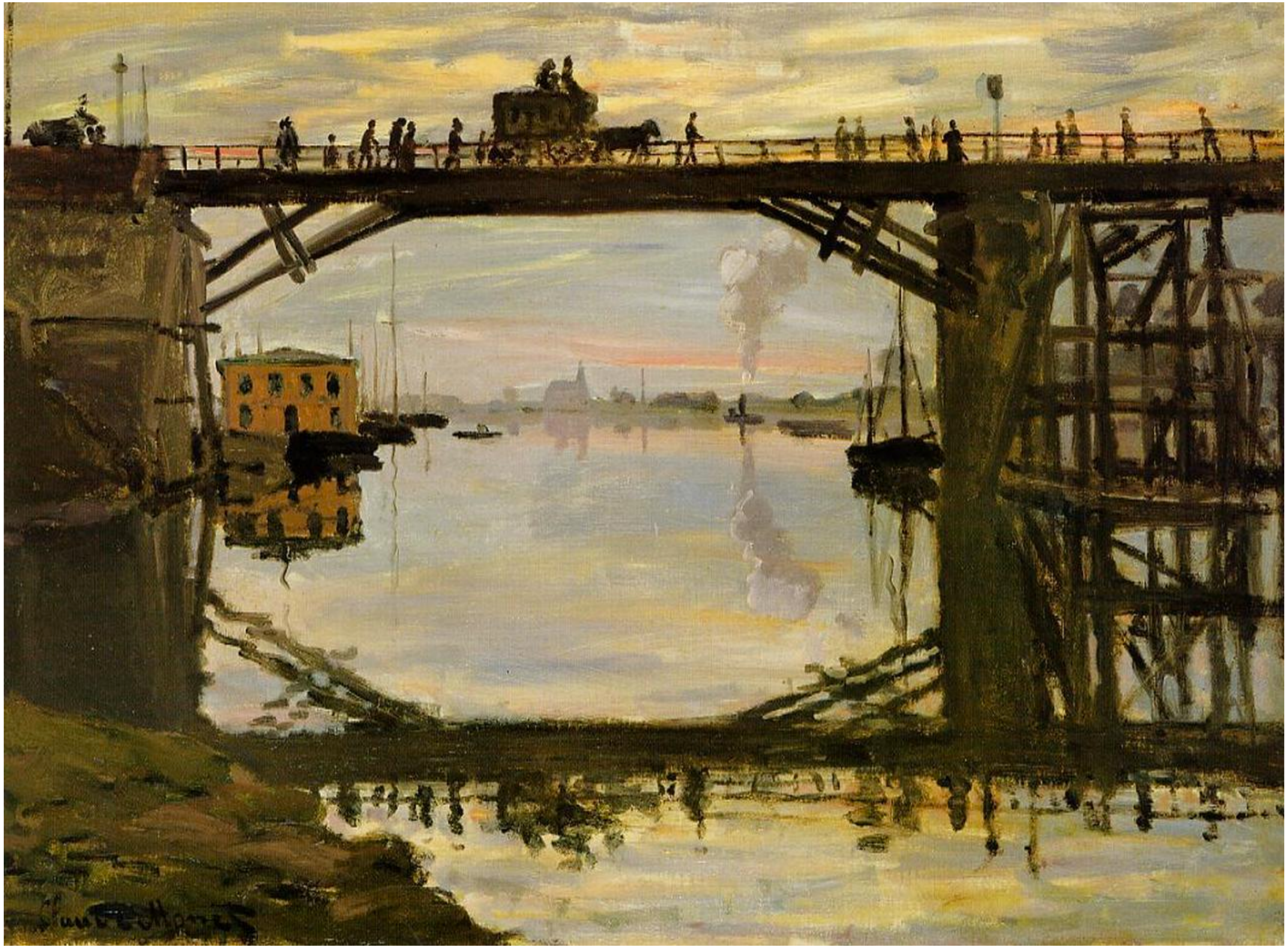
# Building Security In

The long-term solution is to **prevent** all exploitable **bugs before deploying**

Avoid the holes to start with!

# Analogy

- How do you **build a bridge** that stands up despite harsh conditions?
  - Heavy use
  - Earthquakes
  - Extreme weather
  - Etc.



# Do not

- Use methods that **fail to incorporate larger lessons** (i.e., from past bridges built and past failures)
- **Use cheap materials** that are unresilient
- Use **unreliable tools** that produce inconsistent results
- Assume that you can do these things and everything will be OK (you can **just patch problems later**)

# Unless you want your bridge to fail

# PL Approach to Security

- A PL researcher is someone who views the **programming language** as having a **central place in solving computing problems**.
    - by developing *general abstractions,* or *building blocks,* for solving problems, or classes of problems.
- PL research considers software **behavior** in a **rigorous and general way**
    - e.g., to *prove* that (classes of) programs enjoy *properties* we want, and/or eschew properties we don't
- PL thus offers a direction for **building security in**

# Outline of 3 days

- Formalize what software behavior is
  - **Operational semantics**

Day 1

- Formalize rules of what constitutes good behavior
  - **Type systems**

Day 2

- Prove that the rules truly enforce good behavior
  - **Type safety**
- Applications: Information flow security
  - **Information flow security**
  - Secure **cloud services**

Day 3