Grey Science

Breaking down boundaries between the security underground and academia

Talks: Academics or Hackers?

SGX Cache Attacks

Turn Speakers to Microphones for Fun and Profit

Breaking a Widely Used Continuous Glucose Monitoring System

One Car, Two Frames: Attacks on Hitag-2 Remote Keyless Entry Systems Revisited

A Timer-Free High-Precision L3 Cache Attack using Intel TSX

DeTor: Provably Avoiding Geographic Regions in Tor

Hacking in Darkness: Return-oriented Programming against Secure Enclaves

Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More

PDF Mirage: Content Masking Attack Against Information-Based Online Services

Understanding the Mirai Botnet

USB Snooping Made Easy: Crosstalk Leakage Attacks on USB Hubs

Offensive Malware Analysis: Dissecting OSX/FruitFly via a Custom C&C Server

Next-Generation Tor Onion Services

Controlling IoT Devices With Crafted Radio Signals

Cisco Catalyst Exploitation

Persisting with Microsoft Office: Abusing Extensibility Options

Deep Neural Networks for Social Stegonography

Trojan-tolerant Hardware & Supply Chain Security in Practice

Putting the Emerging “Drone Defense” Market to the Test

Talks: Academics or Hackers?

SGX Cache Attacks

Turn Speakers to Microphones for Fun and Profit

Breaking a Widely Used Continuous Glucose Monitoring System

One Car, Two Frames **Keyless Entry Systems Revisited**

A Timer-Free High-Pr **g Intel TSX**

DeTor: Provably Avoi **Tor**

Hacking in Darkness: **ng against Secure Enclaves**

Computer Security, P **Compromising Computers**

with Synthesized DNA, Privacy Leaks, and More

PDF Mirage: Content Masking Attack Against Information-Based Online Services

Understanding the Mirai Botnet

USB Snooping Made Easy: Crosstalk Leakage Attacks on USB Hubs

USENIX Security

Offensive Malware Analysis: Dissecting OSX/FruitFly via a Custom C&C Server

Ne

Cc adio Signals

DEFCON

Ci

Persisting with Microsoft Office: Abusing Extensibility Options

Deep Neural Networks for Social Stegonography

Trojan-tolerant Hardware & Supply Chain Security in Practice

Putting the Emerging "Drone Defense" Market to the Test

Academic and Non-Academic Security and Privacy research has become indistinguishable from one another.

What if the two sides cooperated?

Why Should You Care?

- Some Thought Provoking Examples
- Obstacles
- Solutions
- A Call for Help!

Grey Literature

- Coined by Charles Auger cataloging WWII intel reports and notes on atomic research
- Material outside normal academic or commercial publishing channels

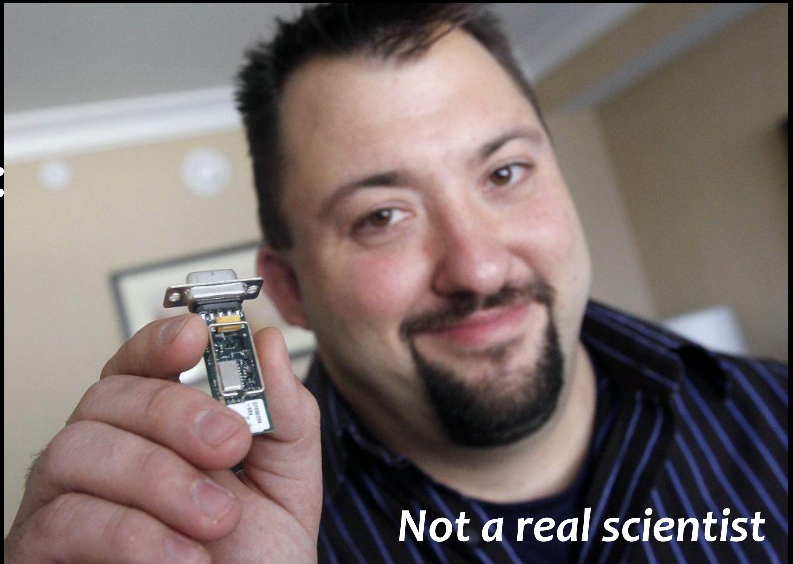
Jay Radcliffe: Hacking His Insulin Pump (2011)

Used the serial number to wirelessly disable, raise and lower insulin

Journals wouldn't publish – no PhD, no MD - "not enough rigor"

"Using the Scientific Method in Security Research" (2017):

Use a methodology – hypothesis, planning, legal advice, experimentation, collect data, disclosure



Not a real scientist

Gregor Mendel, Father of Genetics

Not a real scientist

- ‘Mendel’s Laws of Inheritance’ - how traits are passed to children

- Published in **1865** *Proceedings of the Brno Natural Sciences Society*

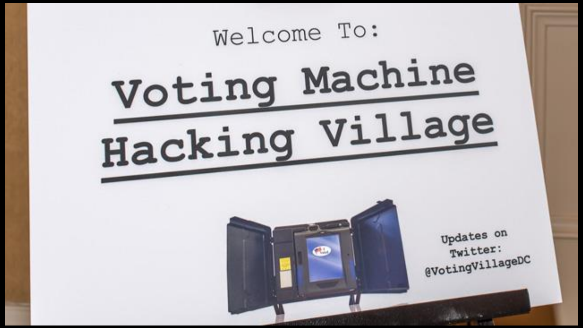
- 1902 Dutch botanist Hugo de Vries is sent the paper by a friend cleaning out old journals.

- **1909** - alleles, zygotes, etc pinned to Mendel

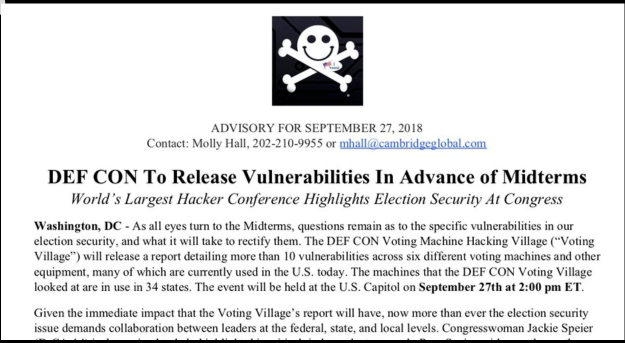
Breaking the boundaries brings success…

DEFCON Voting Village 2017-18

- Academics/Government/Hackers/Kids



- Professional report, Congressional hearings, PR aimed at general public
- Academics: “We’ve known this for years! This Isn’t New!”



ADVISORY FOR SEPTEMBER 27, 2018
Contact: Molly Hall, 202-210-9955 or mhall@cambridgeglobal.com

DEF CON To Release Vulnerabilities In Advance of Midterms

World’s Largest Hacker Conference Highlights Election Security At Congress

Washington, DC - As all eyes turn to the Midterms, questions remain as to the specific vulnerabilities in our election security, and what it will take to rectify them. The DEF CON Voting Machine Hacking Village (“Voting Village”) will release a report detailing more than 10 vulnerabilities across six different voting machines and other equipment, many of which are currently used in the U.S. today. The machines that the DEF CON Voting Village looked at are in use in 34 states. The event will be held at the U.S. Capitol on **September 27th at 2:00 pm ET**.

Given the immediate impact that the Voting Village’s report will have, now more than ever the election security issue demands collaboration between leaders at the federal, state, and local levels. Congresswoman Jackie Speier

Security “Valley of Death” Isn’t New

- Many companies are eliminating research - $$$$

- Federally funded security and privacy research is incremental. Published research is designed to prevent ‘paradigm shifts’

Informal Crowdsourcing of this Idea: ~70% YES/30% NO

- Academics:
  - “It would ruin my credibility”
- Industry:
  - “We just want to get good intellectual property”
- Underground:
  - “Call it ‘experimental science’ vs ‘hacker’ or underground .”
  - “What is research and science anyway? As long as we agree that the basis is experimentation who cares who does it?”
- Government Funders:
  - “If you could ensure no damage, it’s a cheap way to get good research!”

Obstacles to Engaging with Academia

- Ethical and Legal:
  - Institutional Review Boards (IRB) still set up for animal research
  - Offensive Research – no!
- Incentives:
  - Tenure = papers at "top conferences" and in journals
  - Self and grad student funding
- Finding Trusted Collaborators:
  - Academic workshops are invitation only
- Failure is BAD

Obstacles to Engaging Non-Academia

- Culture:
  - Personal satisfaction / challenge vs official collaboration
  - Subset attends in-person gatherings

- Legal:
  - Responsible disclosure standards not clear

What’s Been Done So Far?

- DARPA Cyber Fast Track (2011-13) - 7 days from proposal to funding
- Experience Track at academic conferences
- Bug Bounties
- I Am The Cavalry – security + safety
- DoD Hack the Pentagon - bug hunt open to vetted security specialists. No communitywide understanding about which activities were acceptable. Oops.

What Can Be Done on the Academic Side?

- Sponsor non-academics to participate in grants
- Undergraduate participation
- DARPA, NSF, DHS, Foundations – include an underground component with oversight by PIs
- Invite non academics to workshops - diverse points of view
- Publish conference papers free

What Can Be Done on the Other Side

- Matchmaking at non-academic Cons
  - Academics need results and techniques of offensive research
  - Education on practical security challenges, usability and tools
- Media training/understanding
- More writing about what didn’t work
- Rigor in informal methods

What Can Be Done On the Government Side?

- Non-academics on Cybersecurity panels:
  - CISOs, Security Engineers, Privacy Officers
- Community Advisory Boards
- Crowdsource research ideas among non-academics
- Clarity around ethical research, CFAA restrictions and offensive research needs

Specifically What More Can be Done?

- Neutral Conference
- Day on front or end of academic or hacker con.
    - Present research and data collection challenges from both sides
- Physical meetings at maker spaces or virtually
- CTFs with academics/hackers as equals – setting up and participating
- Engage legal community to jointly address challenges

Journals

- Existing: "International Journal of Proof-of-Concept or Get The F*&^ Out (PoC||GTFO)"
- 2018 ACM Digital Threats, Research and Practice (DTAP)
- New one?

Ideal Model: Biohacking/Quantified Self/DIY Bio

- FBI started contacting DIY Bio groups - concern about synthetic biology

- Jason Bobe, DIYbio.org: “discussions between the community and the FBI have educated both sides. “[FBI agents] need to be educated about the realities of the community and new technologies… it became obvious that we are not the enemy”.

DEFCON 2019 – AI Village Planning

- Seek meaningful research challenge – ie role of AI in Information manipulation
    - Deep Fake video identification/creation in near real time - observe how it goes viral
    - “Fake news” identification
    - Other challenges?
- Goal: Motivate accountability and legislation around online platforms

Comments, thoughts, ideas?
AI Village needs help!

anikolich@iit.edu