WPI

“Everything you always wanted to know about digital forensics*

*But were afraid to ask”

Robert J. Walls


INTEREST

SHERLOCK


SI:NY
THE EIGHTH SEASON)


4210 ½ GRA
4210 ½ GRA
COMPUTER FORMS
BOX 1
11-3-97

Digital Forensics contends with the CSI-Effect

Digital forensics lacks a solid scientific foundation

Digital forensics struggles with practical challenges

Digital forensics impacts people directly

Security != Forensics

Security & Privacy

Security & Privacy & Forensics

5 lessons for researchers

Digital forensics is investigator-centric

1

1. Digital Forensics is Investigator-Centric

- Research is investigator driven.
- Consider both goals and constraints.
- Break the rules lose the case.
- The rules change.

Forensics and law are inseparable

2

2. Forensics and law are inseparable

- Law is struggling to keep up.
- How does seizure apply to data?
- How does plain view apply?
- Forced Decryption?
- Government Hacking?
- Password Sharing?

Investigations are about people

3

3. Investigations are about people

- Focus on the person, not the machine.
- Intent is outside of security domain.
- Consider both computer and traditional crimes.
- Crime may not violate security.

Still useful to catch the dumb ones

4

4. Still useful to catch the dumb ones

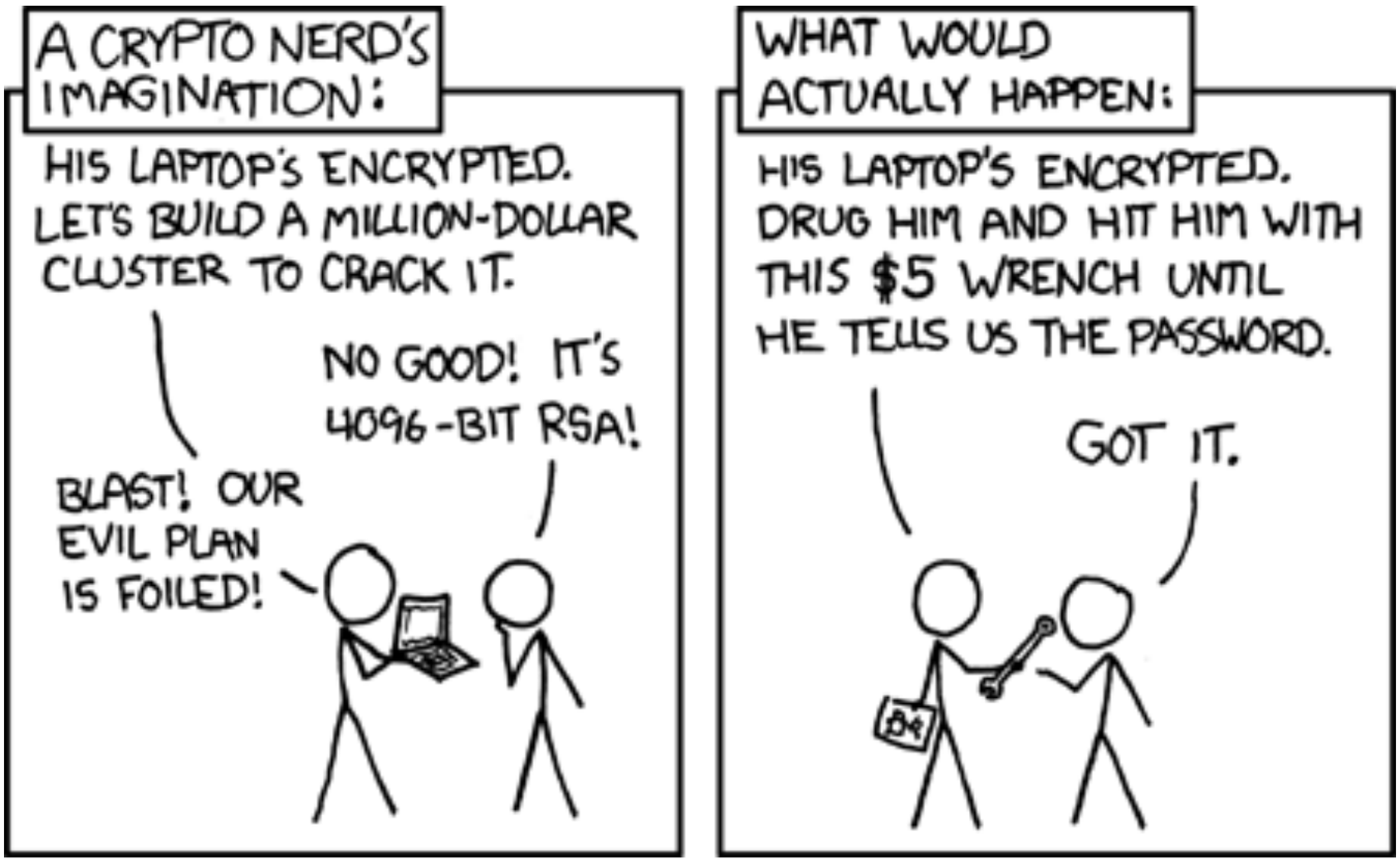
- Doesn’t have to be foolproof to be useful.
- Tech savvy criminals aren’t more dangerous.
- 40% is still good.

Keep it simple

5

5. Keep it simple

- Make it simple for investigators to use it.
- Must be within Investigator capabilities.
- Often simpler non-computer solutions.


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

1: Forensics is Investigator-Centric.

2: Forensics and law are inseparable.

3: Investigations are about people.

4: Still useful to catch the dumb ones.

5: Keep it simple.

Forensics research without these principles is not forensics

What’s next?

Questions?

Robert Walls
rjwalls@wpi.edu