Closing Remarks

Yu Zhang

HIT/CST/NIS

Cryptography, Autumn, 2014

Provable Security

- A proof of security never proves security in an absolute sense, it relates security to an unproven assumption that some computational problem is hard.
- The quality of a security reduction should not be ignored – it matters how tight it is, and how strong the underlying assumption is.
- A security reduction only proves something in a particular model specifying what the adversary has access to and can do.

Crypto Pitfalls

Crypto deceptively simple

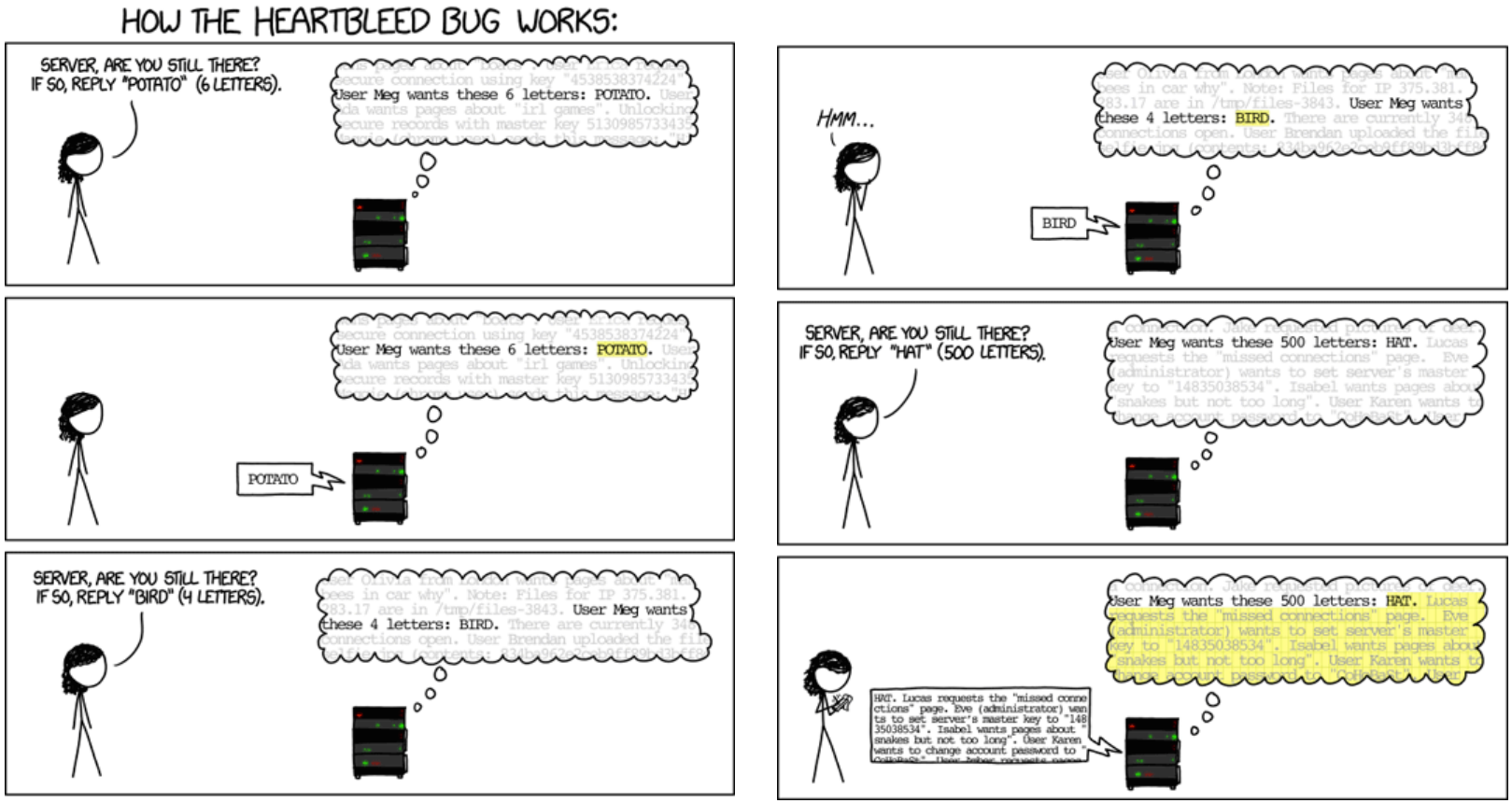
- Why does it so often fail?

Important to distinguish various issues:

1. Bad cryptography/implementations/design, etc.
2. Good cryptography can be 'circumvented' by adversaries operating 'outside the model'
3. Even the best cryptography only shifts the weakest point of failure to elsewhere in your system
4. Systems are complex: key management; social engineering; insider attacks

Avoid the first; be aware of 2-4.

Bad Implementation Example: Heartbleed



Crypto is difficult to get right

- Must be implemented correctly
- Must be integrated from the beginning, not added on "after the fact"
- Need expertise; "a little knowledge can be a dangerous thing"
- Can't be secured by Q/A, only (at best) through penetration testing and dedicated review of the code by security experts

General Recommendation

- Use only standardized algorithms and protocols
- No security through obscurity!
- Use primitives for their intended purpose
- Don't implement your own crypto
- If your system cannot use "off-the-shelf" crypto components, re-think your system
- If you really need something new, have it designed and/or evaluated by an expert
- Don't use the same key for multiple purposes
- Use good random-number generation

Crypto Libraries

- Use existing, high-level crypto libraries: cryptlib, NaCl, Google's Keyczar, Mozilla's NSS, OpenSSL
- Avoid low-level libraries (like JCE, crypto++, GnuPG, OpenPGP) - too much possibility of mis-use
- Avoid writing your own low-level crypto

Beware of Snake Oil

Snake Oil: bogus commercial cryptographic products.

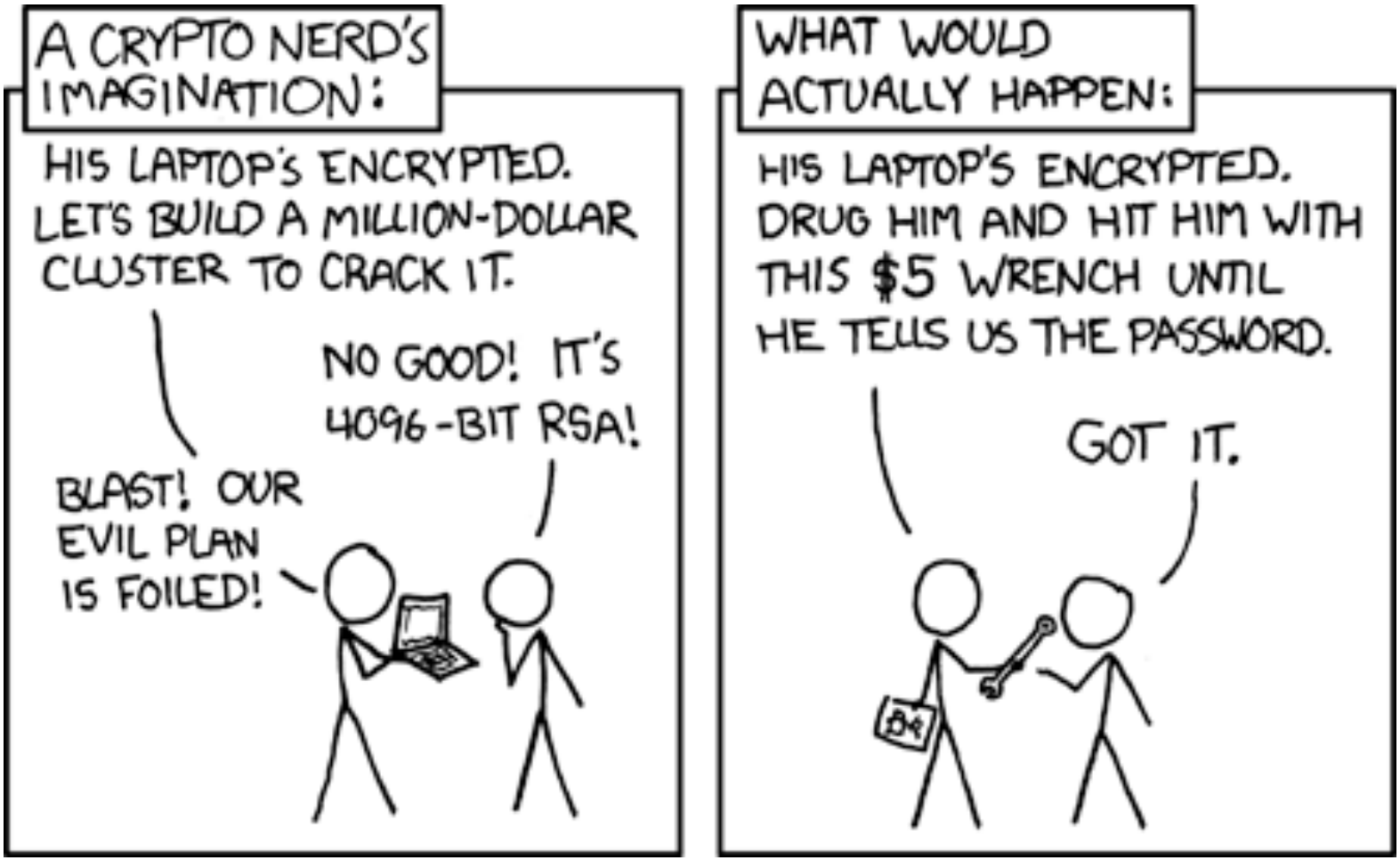
- **Secret system**: security through obscurity
- **Technobabble**: since cryptography is complicated
- **Unbreakable**: a sure sign of snake oil
- **One-time pads**: a flawed implementation
- **Unsubstantiated "bit" claims**: key lengths are not directly comparable

What cryptography can and can't do

"No one can guarantee 100% security. But we can work toward 100% risk acceptance. ... Strong cryptography can withstand targeted attacks up to a point–the point at which it becomes easier to get the information some other way. ... The good news about cryptography is that we already have the algorithms and protocols we need to secure our systems. The bad news is that that was the easy part; implementing the protocols successfully requires considerable expertise. ... Security is different from any other design requirement, because functionality does not equal quality."

– By Bruce Schneier 1997

Rubber-hose Cryptanalysis



A Good Wish

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

– Article 12 Universal Declaration of Human Rights