Cryptoparty

redshiftzero
jen@redshiftzero.com

Southside Hackerspace: Chicago

October 4, 2014

What are we going to do today?

- Introductions
- Context
- Basic cryptography/security concepts
- Setting up tools: PGP for email encryption
- Open time: Q and A, lightning talks, keysigning
- Already use PGP? Please help teach!

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.
- You may not have anything to hide, but the government may think you do: e.g. bloated terrorist watch lists that are hard to remove oneself from.

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.
- You may not have anything to hide, but the government may think you do: e.g. bloated terrorist watch lists that are hard to remove oneself from.
- Are you sure you have nothing to hide? There are lots of laws.

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.
- You may not have anything to hide, but the government may think you do: e.g. bloated terrorist watch lists that are hard to remove oneself from.
- Are you sure you have nothing to hide? There are lots of laws.
- People hide many things even though they're not wrong. e.g. nudity

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.
- You may not have anything to hide, but the government may think you do: e.g. bloated terrorist watch lists that are hard to remove oneself from.
- Are you sure you have nothing to hide? There are lots of laws.
- People hide many things even though they're not wrong. e.g. nudity
- You may not care about hiding it, but you may still be discriminated against because of it. e.g. a company decides that statistically a behavior might suggest you are a poor risk

Why should we care about privacy?

- Some people have something to hide, but not something the government should have the power to know: e.g. affairs, being in the closet, medical information.
- You may not have anything to hide, but the government may think you do: e.g. bloated terrorist watch lists that are hard to remove oneself from.
- Are you sure you have nothing to hide? There are lots of laws.
- People hide many things even though they're not wrong. e.g. nudity
- You may not care about hiding it, but you may still be discriminated against because of it. e.g. a company decides that statistically a behavior might suggest you are a poor risk
- Privacy is important for dissidents and democracy. It helps maintain the balance of power between individuals and the state.

Lessons from Snowden

- The NSA is grabbing up lots of data. Their motivation is to collect every communication that exists, everywhere.

Lessons from Snowden

- The NSA is grabbing up lots of data. Their motivation is to collect every communication that exists, everywhere.
- "Properly implemented strong cryptosystems are one of the few things we can rely on"

Lessons from Snowden

- The NSA is grabbing up lots of data. Their motivation is to collect every communication that exists, everywhere.
- "Properly implemented strong cryptosystems are one of the few things we can rely on"
- But endpoint security is an issue.

Lessons from Snowden

- The NSA is grabbing up lots of data. Their motivation is to collect every communication that exists, everywhere.
- "Properly implemented strong cryptosystems are one of the few things we can rely on"
- But endpoint security is an issue.
- If the government and corporations don't care about protecting our privacy, we can do it for ourselves.

Security Mindset

There's no such thing as absolute security. Consider your home.

You're balancing risk and security. You want to exert just more effort than your adversary is willing to commit.

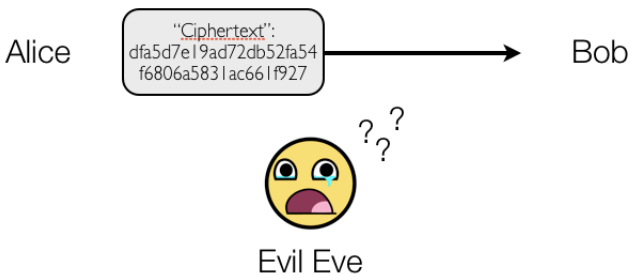
Consider your threat model:

- **What do you want to keep private?** e.g. your .porn directory, your stolen government documents, the fact that you have cancer, your sexuality
- **Who wants to know?** e.g. Your employer? Nosy kids in coffee shops? Criminals? Police? FBI? NSA?
- **What can they do to find out?** e.g. Dragnet surveillance vs. targeted surveillance, subpoena third parties for your data, hack into your computers
- **What happens if they succeed?** e.g. embarassment to death, imprisonment

Then you make a security plan.

How can we communicate securely in the presence of third parties? Cryptography!

How can we communicate securely in the presence of third parties? Cryptography!



General Computer Security Advice

- Keep your system (both your OS and applications) up to date with security updates.

General Computer Security Advice

- Keep your system (both your OS and applications) up to date with security updates.
- Don't run code from people or organizations you don't trust: Email attachments!

General Computer Security Advice

- Keep your system (both your OS and applications) up to date with security updates.
- Don't run code from people or organizations you don't trust: Email attachments!
- Free and open source software is better for security: Linux!

General Computer Security Advice

- Keep your system (both your OS and applications) up to date with security updates.
- Don't run code from people or organizations you don't trust: Email attachments!
- Free and open source software is better for security: Linux!
- Don't reuse passwords if possible, use long passwords, and use two-factor authentication if available. Use a password manager if that helps (e.g. Keepass).

General Computer Security Advice

- Keep your system (both your OS and applications) up to date with security updates.
- Don't run code from people or organizations you don't trust: Email attachments!
- Free and open source software is better for security: Linux!
- Don't reuse passwords if possible, use long passwords, and use two-factor authentication if available. Use a password manager if that helps (e.g. Keepass).
- Use HTTPS as much as possible: Install **HTTPS Everywhere**, a browser extension.