SECURITY BY & FOR FREE SOFTWARE

RYAN PRIOR

ABOUT THIS TALK

Freedom & security are mutually dependent

What undermines one, undermines the other

MY BACKGROUND

I'm Ryan Prior

Security engineering at CyberArk
I help organizations build defensible systems

Related note: I developed this talk on work time!

THINGS I'M NOT COVERING...

THINGS I'M NOT COVERING...

- Detection (intrusions, malware)

THINGS I'M NOT COVERING...

- Detection (intrusions, malware)
- Securing your application

THINGS I'M NOT COVERING...

- Detection (intrusions, malware)
- Securing your application
- Everything that's wrong with security today

THINGS I WILL COVER...

THINGS I WILL COVER...

- Defense in-depth

THINGS I WILL COVER...

- Defense in-depth
- Current environment

THINGS I WILL COVER...

- Defense in-depth
- Current environment
- Systems thinking

DEFENSE IN-DEPTH

- Principle of least authority
- Granular data access
- Healthy boundaries

PRINCIPLE OF LEAST AUTHORITY

No agent is over-authorized

(where an agent is a user, machine, or process)

GRANULAR DATA ACCESS

Access is specific

Agents have only what they need right now

HEALTHY BOUNDARIES

When an agent is inevitably compromised, boundaries contain the impact

STATUS QUO, EXTREMELY OVERSIMPLIFIED

Strategy: keep bad actors out

When that fails… ¯_(ツ)_/¯

DEALING WITH HIJACKERS

…in the bad old days

THE 9/11 PRINCIPLE

Don't let just anybody fly the plane!

Try to prevent a bad actor from getting access…
Be prepared to resist them when they do

SECURITY DESPAIR

- Badger people to adopt practices
- Create anxiety about security
- Warn of dire consequences
- Compare security to the punishment of Sisyphus

SECURITY DESPAIR

- Badger people to adopt practices
- Create anxiety about security
- Warn of dire consequences
- Compare security to the punishment of Sisyphus

SECURITY DESPAIR

- Badger people to adopt practices
- Create anxiety about security
- Warn of dire consequences
- Compare security to the punishment of Sisyphus

SECURITY DESPAIR

- Badger people to adopt practices
- Create anxiety about security
- Warn of dire consequences
- Compare security to the punishment of Sisyphus

SECURITY DESPAIR

- Badger people to adopt practices
- Create anxiety about security
- Warn of dire consequences
- Compare security to the punishment of Sisyphus

SECURITY EXPERTS WILL FOREVER SHOUT INTO THE VOID AND OTHERS WILL FOREVER IGNORE THEIR ADVICE

SOME INSPIRATION!

- One computer for games, another for work
- Webserver admins limit access to `www` user
- Web browsers isolate each tab
- `root` owns system files

SYSTEMS THINKING

individual practices → collective principles
application features → platform guarantees
securing programs → defensible system

DISCOVERY & INSTALLATION

Discover & try new things, quickly, confidently

Handcrafted sandboxing → automatic isolation

PRIVACY

Automate storage and handling of sensitive info

Handcrafted data handling → managed data lifecycle

PASSWORDS & CO.

People want to move on from managing secrets!

Passwords, keys, certificates → uniform access control

PASSWORDS & CO.

People want to move on from managing secrets!

Passwords, keys, certificates → uniform access control

these things may continue to exist;
the user must not manage them

SOCIAL MACHINES

- live collaboration
- deep sharing
- access control

Managing files → social computing

SOCIAL MACHINES

- live collaboration
- deep sharing
- access control

Managing files → social computing

SOCIAL MACHINES

- live collaboration
- deep sharing
- access control

Managing files → social computing

SOCIAL MACHINES

- live collaboration
- deep sharing
- access control

Managing files → social computing

DRIVING ADOPTION

Appeal to self-interest of:

- application developers
- maintainers
- end users

A PLATFORM IS NOT

- a framework
- a programming language
- a bandage

SECURING YOUR DESKTOP

SECURING YOUR DESKTOP

- BitWarden - password manager

SECURING YOUR DESKTOP

- FlatPak/Snap - sandboxed application pods

SECURING YOUR DESKTOP

- SubgraphOS - automatic sandboxing of applications

SECURING YOUR DESKTOP

- QubesOS - domain separation using VMs

SECURING YOUR DESKTOP

- SilverBlue - immutable OS

SECURING YOUR MOBILE

SECURING YOUR MOBILE

- BitWarden (again!)

SECURING YOUR MOBILE

- Orbot - route all traffic through Tor

SECURING THE CLOUD

SECURING THE CLOUD

- NextCloud - consumer cloud services

SECURING THE CLOUD

- CloudFoundry - deploy code to create a service

SECURING THE CLOUD

- Conjur - automated password manager for machines

SECURING THE CLOUD

- Envoy - network isolation & service discovery

SECURING THE CLOUD

- Secretless - remove passwords & secrets from applications

THINGS WE COVERED

- Security and freedom are mutually dependent
- Systems thinking is a path out of despair
- Security is aligned with other interests
- Hackers & maintainers can get involved

THANK YOU!

Send comments to:
ryanprior@mastodon.social
@ryanprior

Fork this talk:
https://gitlab.com/ryanprior/security-freedom-talk

Please give me your questions!