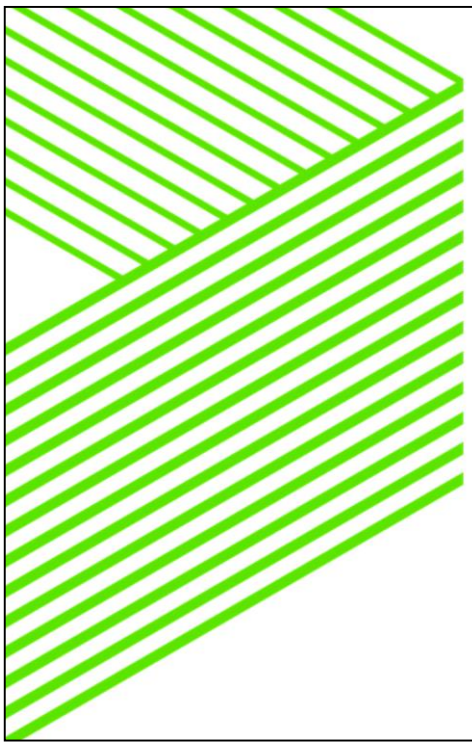


PUG CHALLENGE EXCHANGE AMERICAS

Securing Legacy Apps – Worth the Effort?

Michael Solomon

29 June 2016

It depends on thoughtful assessment of your application and its vulnerabilities

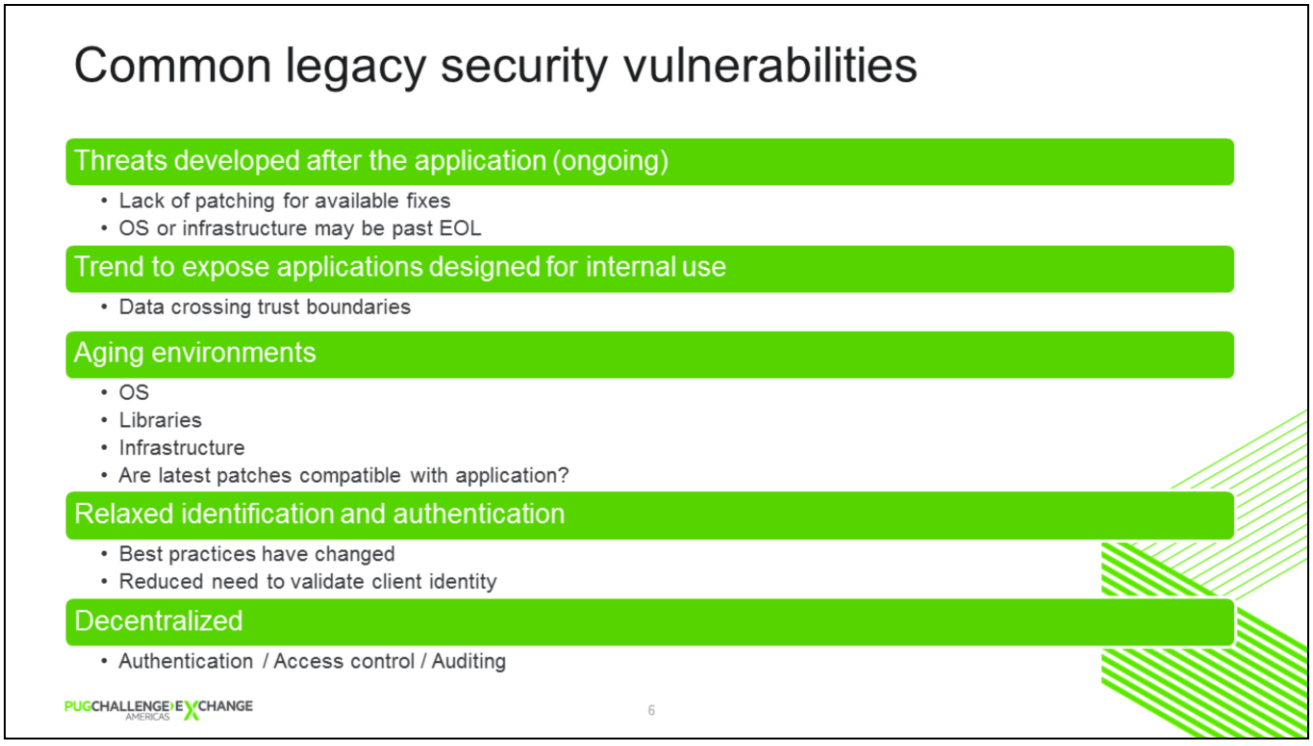
Agenda

- What is a legacy application?
- How are they vulnerable?
- What can we do about it?
- Where can I get help?

You do have AT LEAST one legacy application, right?

Legacy security often relied on physical barriers.

Physical controls protected data.



These are just the most common reasons that legacy applications have security vulnerabilities.

Legacy client types

Terminal systems

- Mainframe
- TTY terminals
- OpenEdge Character (CHUI) client

Client/Server

- Workstation
- Networked connection to database
- OpenEdge GUI client

Browser

- Internet application
- Runs in web browser
- OpenEdge WebSpeed

Terminal system application vulnerabilities

Authentication often depends on OS

Authorization based on file system permissions

*** Limited or nonexistent encryption capability ***

in-transit/at rest

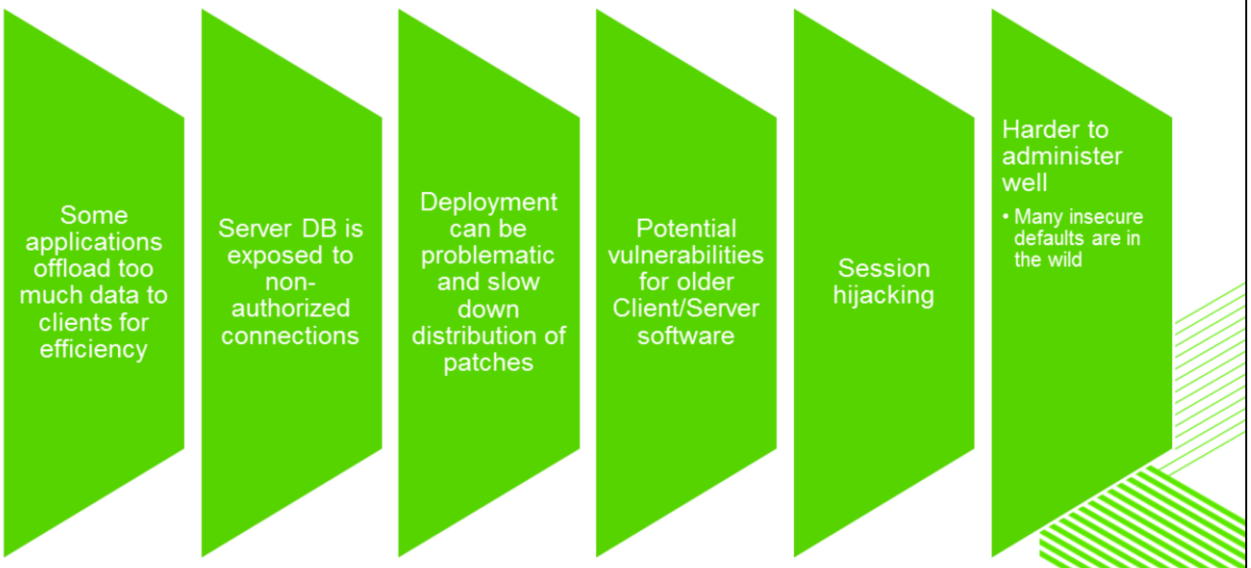
No local input data validation

Often dependent on physical terminal characteristics (perhaps for input validation)

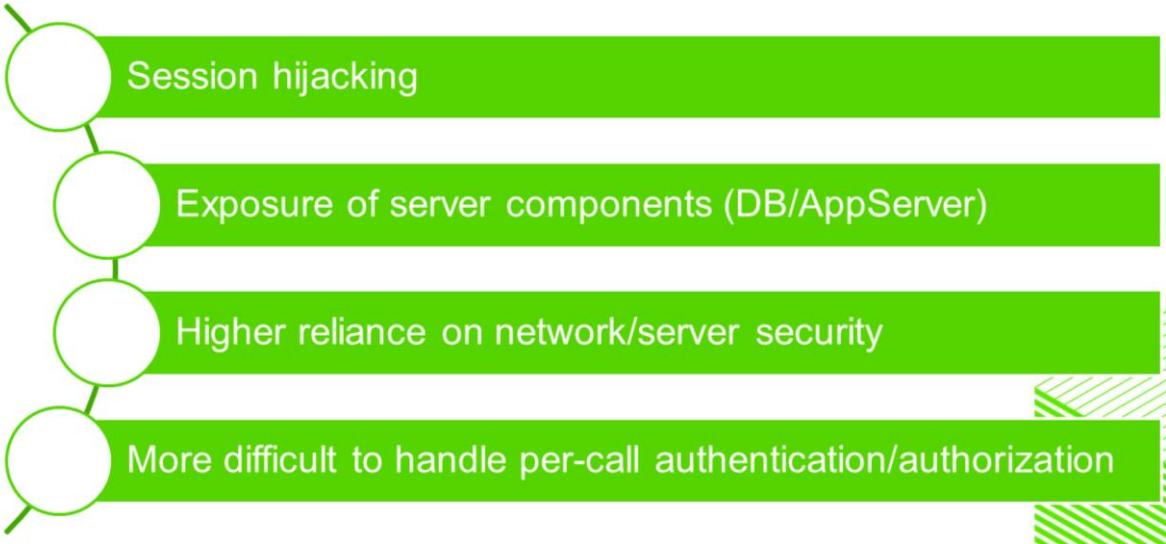
Due to historical physical separation security

- other areas may be sloppy (i.e. hardcoded userids/passwords)

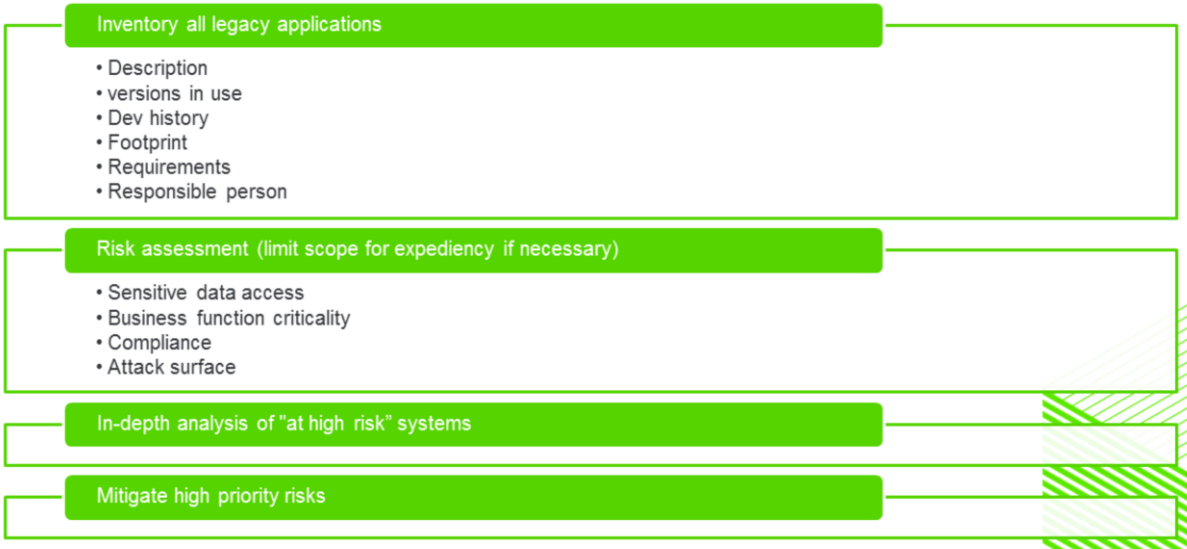
Client/Server application vulnerabilities



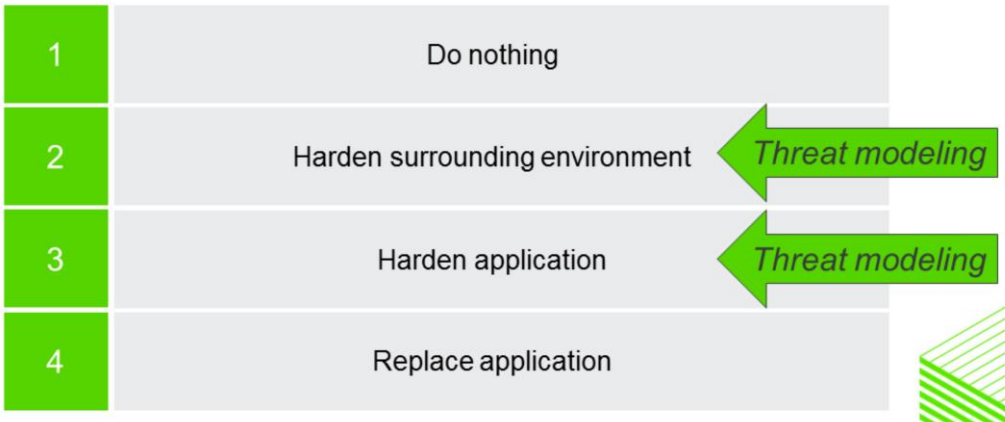
Browser application vulnerabilities

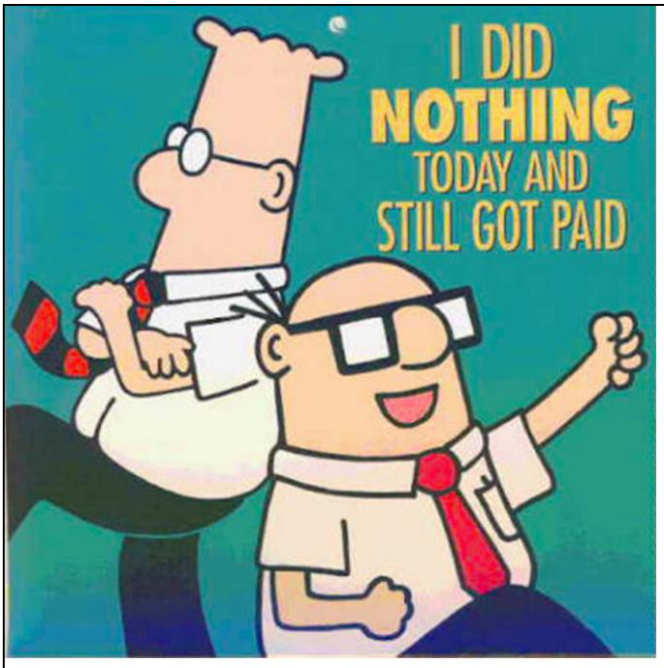


What does it take to secure legacy applications?



Mitigation options

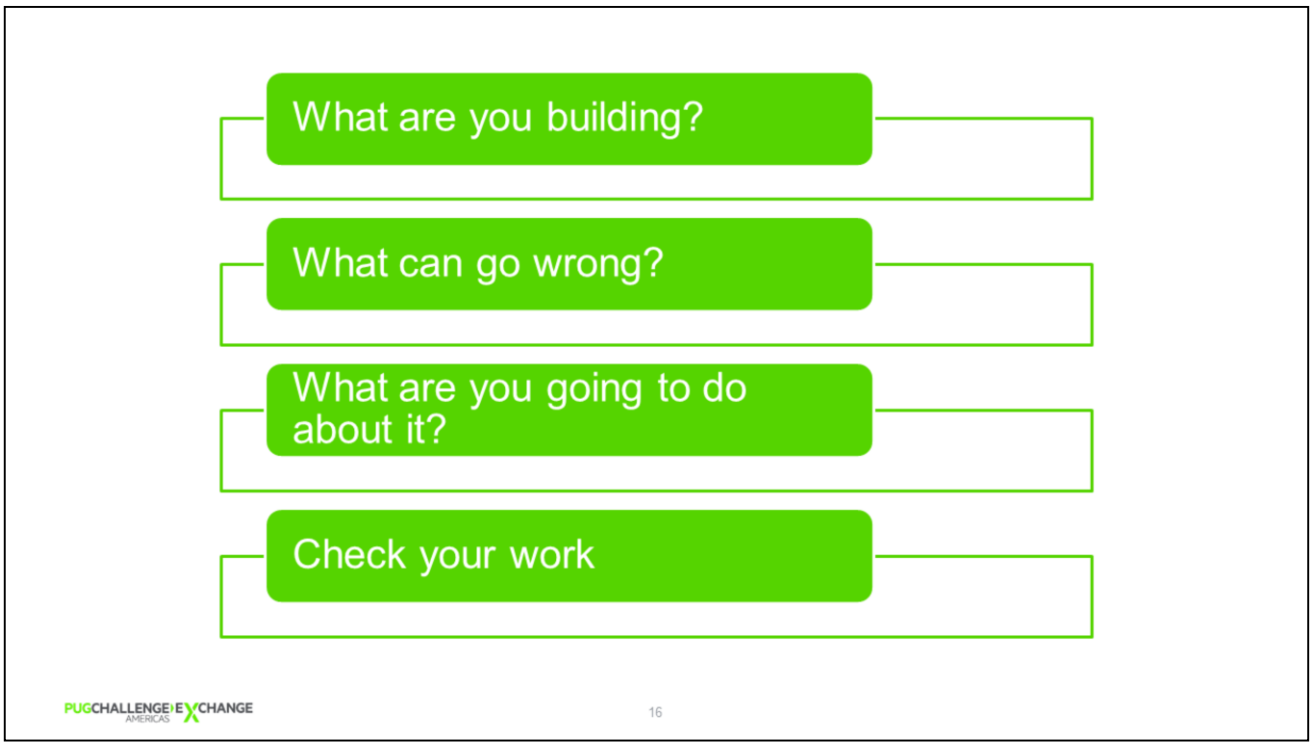




- May be the best choice
- Risk assessment provides response recommendations
- Better than wasting resources on ineffective controls
- Choose this option
  - Don't default to it


Manage risk with threat modeling


How to threat model


What are you building?
What can go wrong?
What are you going to do about it?
Check your work
PUGCHALLENGE EXCHANGE
AMERICAS
16

What are you building?

Create a system model

- Abstracts away the details

Diagrams are key

- Mathematical models are rare in industry

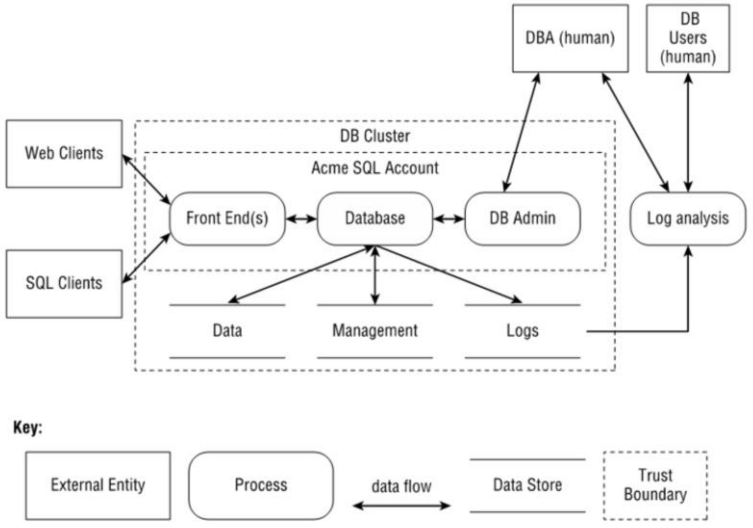
Primary focus in threat modeling

- Data flows
- Threat boundaries

Common diagram types

- Data Flow Diagrams (DFD)
- Swim Lanes
- State machines

Data Flow Diagram

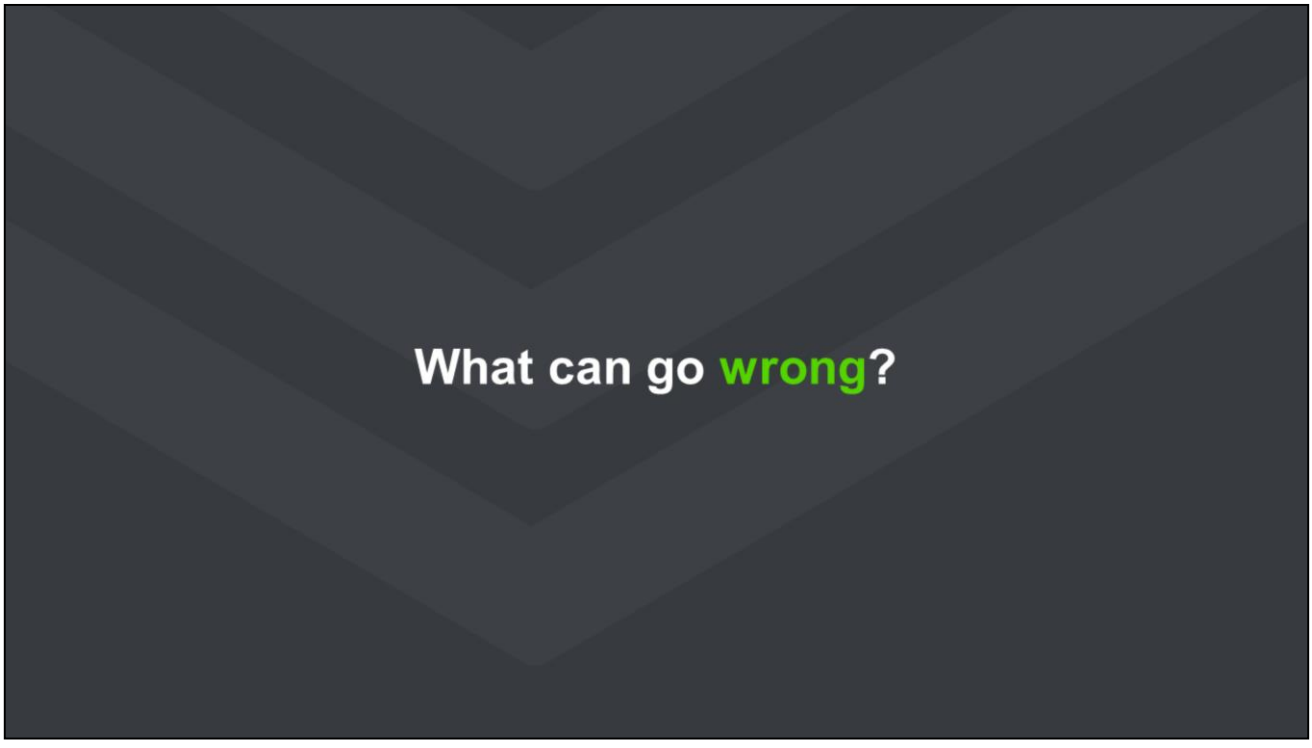


Developed in the early 70s, and still useful

- Simple: easy to learn, sketch
- Threats often follow data

Abstracts programs into:

- Processes: your code
- Data stores: files, databases, shared memory
- Data flows: connect processes to other elements
- External entities: everything but your code & data. Includes people & cloud software
- Trust boundaries now made explicit



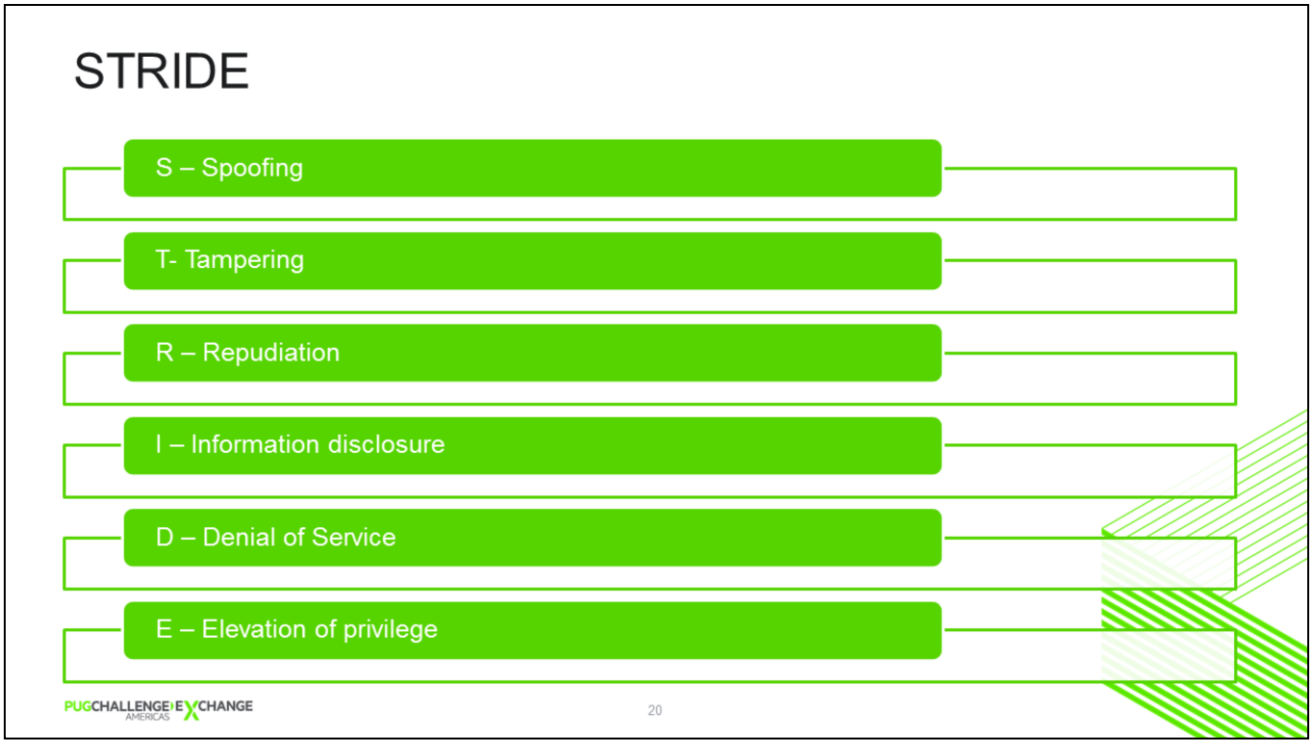
Fun to brainstorm

Mnemonics, trees or libraries of threats can all help structure thinking

Structure helps get you towards completeness and predictability

STRIDE is a mnemonic

> Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
>
> Easy, right?


STRIDE
S – Spoofing
T- Tampering
R – Repudiation
I – Information disclosure
D – Denial of Service
E – Elevation of privilege
PUGCHALLENGE EXCHANGE
AMERICAS
20

Threat	Property Violated	Definition	Example
Spoofing	Authentication	Impersonating something or someone else.	Pretending to be any of Bill Gates, Paypal.com or ntdll.dll
Tampering	Integrity	Modifying data or code	Modifying a DLL on disk or DVD, or a packet as it traverses the network
Repudiation	Non-repudiation	Claiming to have not performed an action.	"I didn't send that email," "I didn't modify that file," "I *certainly* didn't visit that web site, dear!"
Information Disclosure	Confidentiality	Exposing information to someone not authorized to see it	Allowing someone to read the Windows source code; publishing a list of customers to a web site.
Denial of Service	Availability	Deny or degrade service to users	Crashing Windows or a web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole.
Elevation of Privilege	Authorization	Gain capabilities without proper authorization	Allowing a remote internet user to run commands is the classic example, but going from a limited user to admin is also EoP.

Using STRIDE

How can each STRIDE threat can impact each part of your model

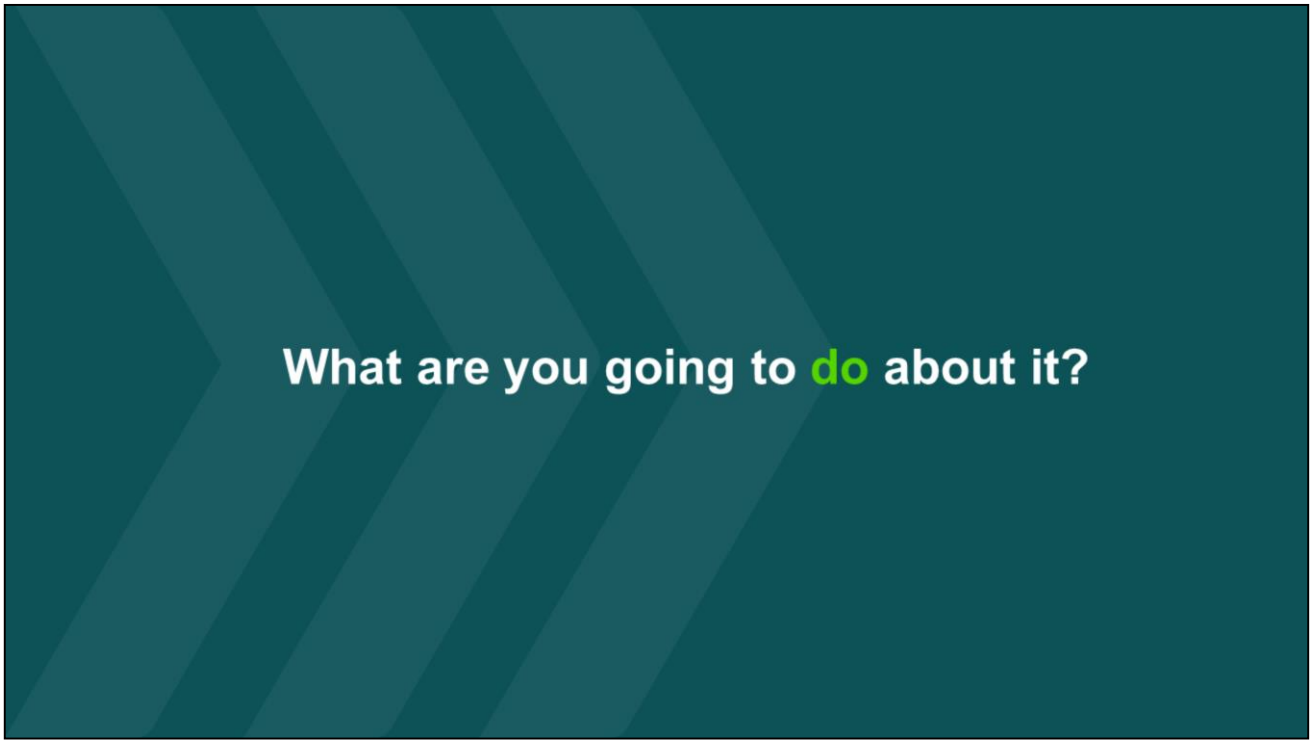
- How could an attacker tamper with this part of the system?

Make it easier

- Elevation of Privilege Game
  - https://www.microsoft.com/en-us/sdl/adopt/eop.aspx
  - https://www.thegamecrafter.com/games/elevation-of-privilege
- Attack Trees
- Experience

Track issues as you find them

- Track assumptions too


What are you going to do about it?

Threats and assumptions

For each threat

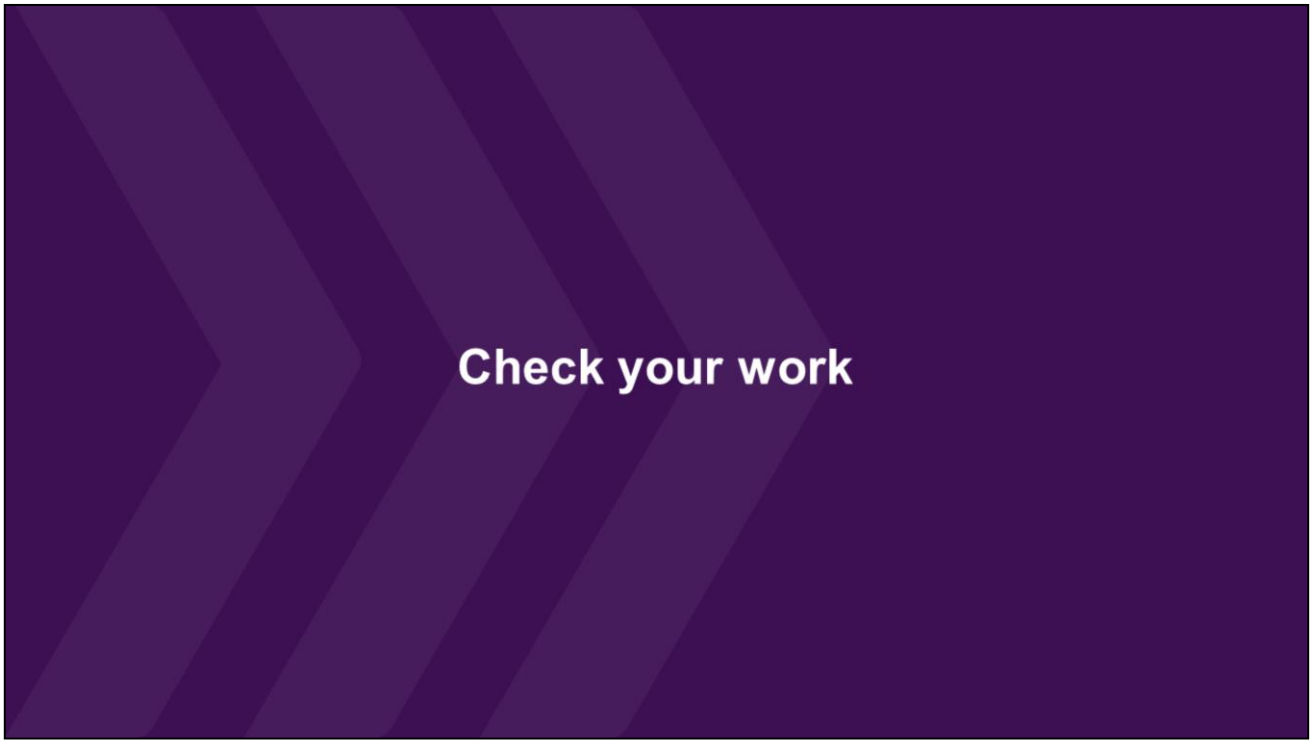
- Fix – remove functionality
- Mitigate
- Accept – Be careful about accepting customer risk
- Transfer – License agreements, TOS

For each assumption

- Check
- Reconsider wrong assumptions

Ways to mitigate threats

Threat	Mitigation Technology	Developer Example	Sysadmin Example
Spoofing	Authentication	Digital signatures, Active directory, LDAP	Passwords, crypto tunnels
Tampering	Integrity, permissions	Digital signatures	ACLs/permissions, crypto tunnels
Repudiation	Fraud prevention, logging, signatures	Customer history risk management	Logging
Information disclosure	Permissions, encryption	Permissions (local), PGP, SSL	Crypto tunnels
Denial of service	Availability	Elastic cloud design	Load balancers, more capacity
Elevation of privilege	Authorization, isolation	Roles, privileges, input validation for purpose, (fuzzing*)	Sandboxes, firewalls



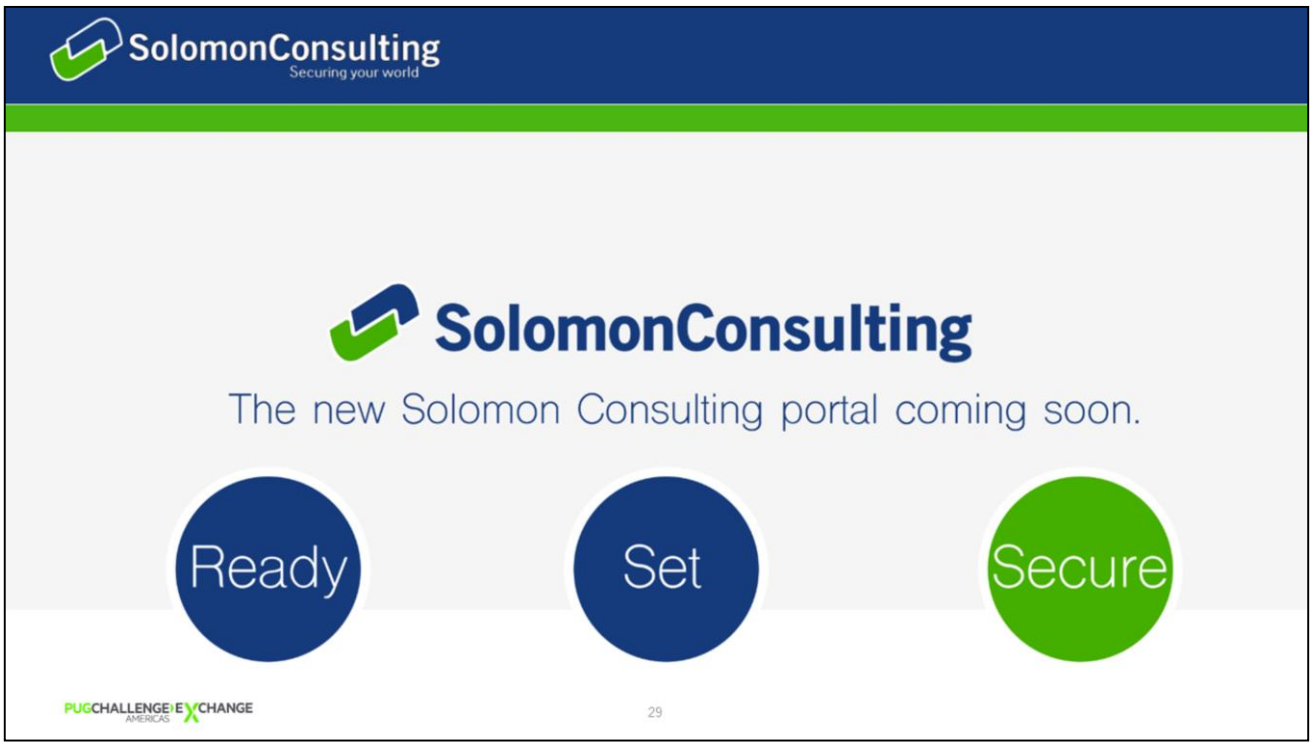
Quality assurance

Check that you covered all the threats & assumptions

Check that each is covered well

Sometimes you just can't mitigate enough vulnerabilities in legacy applications.

Replace software when mitigation cost is too high and replacement software meets needs



www.solomonconsulting.com

References

- https://buildsecurityin.us-cert.gov/articles/best-practices/legacy-systems/assessing-security-risk-in-legacy-systems
- http://www.computerworld.com/article/2474158/application-security/4-risks-from-legacy-applications.html
- http://www.csoonline.com/article/2139382/data-protection/forgotten-risks-hide-in-legacy-systems.html
- https://securityintelligence.com/what-are-the-risks-of-legacy-infrastructure/
- http://www.codingthearchitecture.com/2015/03/07/security_concerns_for_legacy_systems.html
- http://www.datacenterjournal.com/securing-legacy-applications-modern-threats/
- https://www.owasp.org/index.php/OWASP_Supporting_Legacy_Web_Applications_in_the_Current_Environment_Project