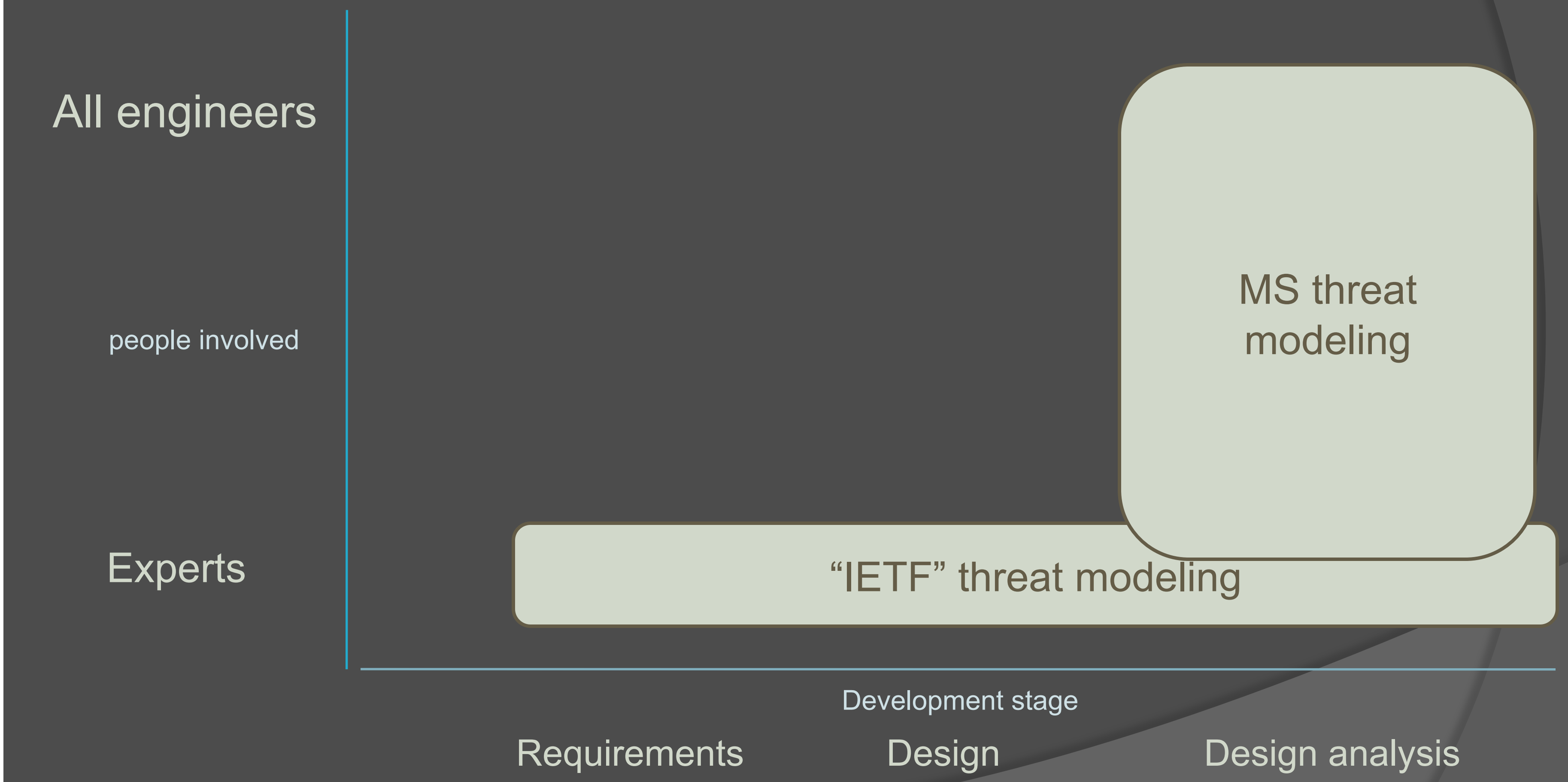
SDL THREAT MODELING: PAST, PRESENT AND FUTURE

Adam Shostack

Microsoft

Terminology & Context



All engineers

people involved

Experts

MS threat modeling

“IETF” threat modeling

Development stage

Requirements

Design

Design analysis

THREAT MODELING:

PAST

Some history

- Almost 10 years of threat modeling
- More than one process developed/year
- Massive profusion of ideas and experiments

Process version history

- 1999 "Threats to Our Software" (Garms, Garg, Howard)
  - Developed STRIDE
- 2001 *Writing Secure Code* (Howard, LeBlanc)
- 2002 *Writing Secure Code,* 2nd edition (Howard, LeBlanc)
  - Wysopal/Howard work integrated @Stake, Microsoft processes
  - Added DREAD
- 2004 Formal rollout of security development lifecycle (SDL)
  - Includes threat model to meet secure-by-design commitment of SD3+C
- 2004 *Threat Modeling* (Swiderski, Snyder)
- 2006 *Security Development Lifecycle,* the book (Howard, Lipner)
- …

Threat modeling issues

- The process is complex
  - Eleven steps
  - " Only works with an expert in the room"
  - Jargon overload
- The process is disconnected from development
- “We’re a component, we don’t have assets”
- Few customers for threat modeling artifacts
  - "Throw it over the wall to security"
- It's hard to tell if the threat model is
  - Complete?
  - Accurate and up-to-date?
- Expensive to do, value not always clear
  - (Especially if you're not sure how to threat model)
- Training
- The list of pain points goes on and on…

“The process that works for me is…”

- SDL process
- *Writing Secure Code* process (Howard and LeBlanc)
- *Threat Modeling* (Swiderski and Snyder, Microsoft Press)
- "Guerilla Threat Modeling" (Peter Torr)
- Patterns and Practices (J.D. Meier)
- Threat modeling for dummies (Larry Osterman)
- Line-of-business threat modeling (ASAP/ACE team)
- Per team
  - MED threat modeling (Matt Lyons)
  - "Creating High-Quality Shell TMAs" (Anil Yadav, Mike Sheldon, Eric Douglas)

Sorry if I missed your version of the process

THREAT MODELING:

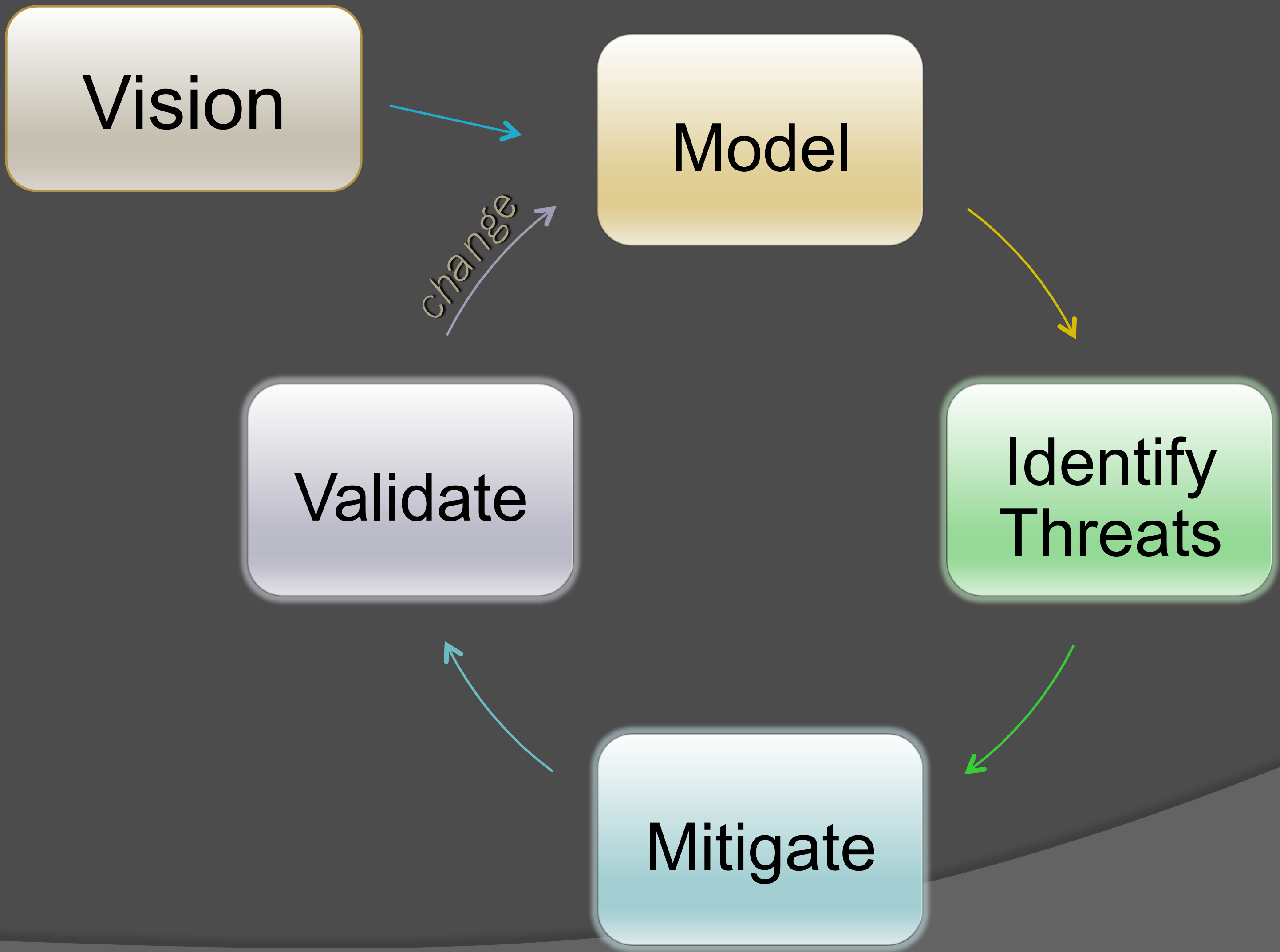
PRESENT

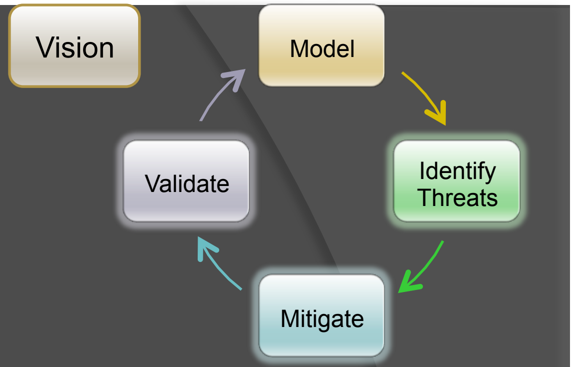
New SDL process addresses many issues

- The process is complex
  - Eleven steps
  - “Only works with an expert in the room"
  - Jargon overload
- The process is disconnected from development
- We’re a component with no assets
- Few customers for threat modeling artifacts
  - "Throw it over the wall to SWI"
- It's hard to tell if the threat model is:
  - Complete?
  - Accurate and up-to-date?
- Expensive to do, value not always clear
  - (Especially if you're not sure how to threat model)
- Training

- Four-step process
- Explicit jargon purge
- Product studio integration
- TM based on software, not attacker
- TM as collaboration tool
- Self-checks in process
- Make it easier
- Threats as bugs
- Mitigations as features
- Better training

Evolved SDL Process

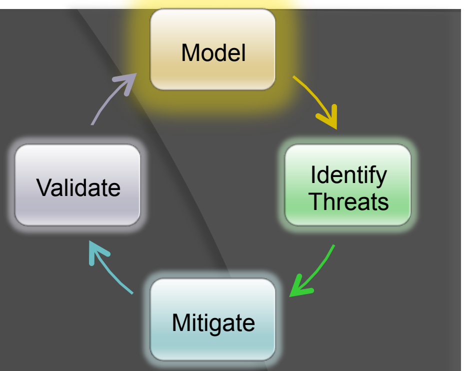




Vision

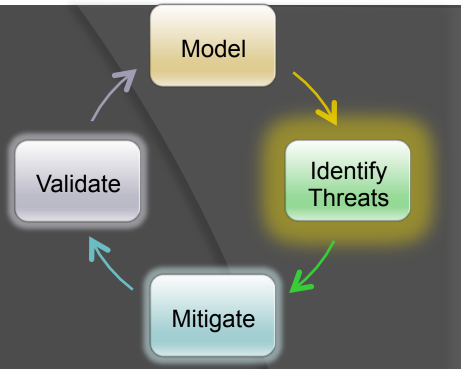
- Scenarios
  - Where do you expect the product to be used?
  - Live.com is different from Vista
  - MLB.com is different from an internal web site
- Use cases/use Stories
- Add security to scenarios, use cases
- Assurances
  - Structured way to think about "what are you telling customers about the product's security?"

Model



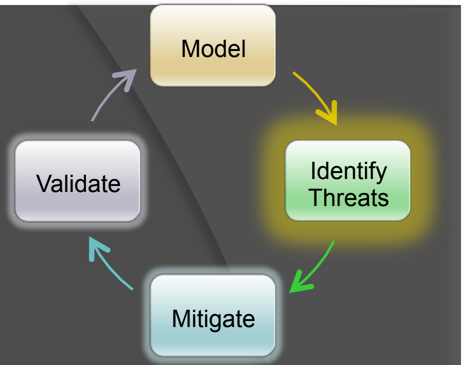
- Start with a overview which has:
  - A few external interactors
  - One or two processes
  - One or two data stores (maybe)
  - Data flows to connect them
- Check your work
  - Does it tell the story at an elevator pitch level?
  - Does it match reality?
- Break out more layers as needed

Identify Threats



- Sounds good, but remember we’re asking all engineers to be involved
- How do you do it if you’re not an expert?
- Requires prescriptive guidance

"STRIDE per Element"


Model

Identify Threats

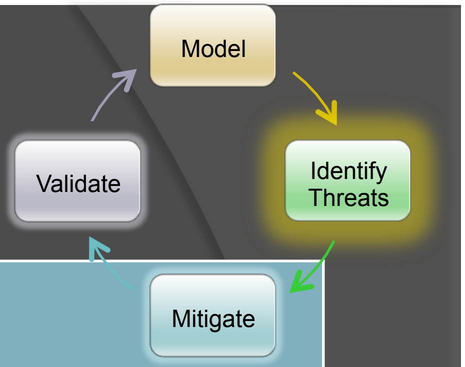
Mitigate

Validate

	Spoofing	Tamper.	Rep.	Info.Disc.	DoS	EoP
External Entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data Store		✓	✓	✓	✓	
Dataflow		✓		✓	✓	

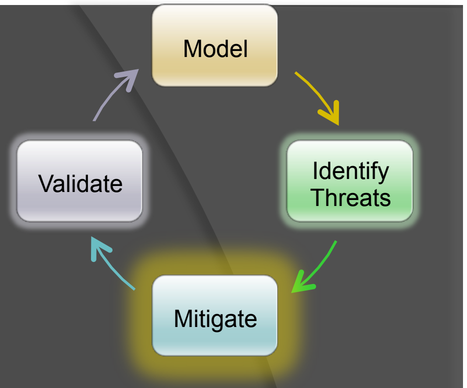
This is our chart; it may not be the issues you need to worry about

Threats & Properties



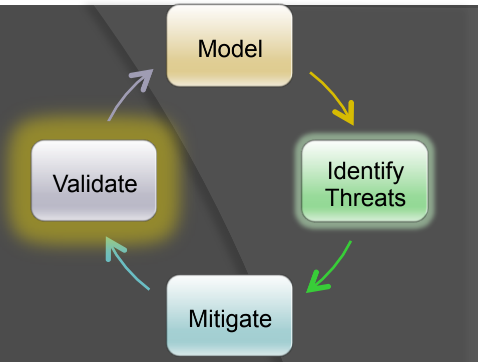
Threat	Property	Definition	Example
Spoofing	Authentication	Impersonating something or someone else.	**Pretending to be any of billg, microsoft.com or ntdll.dll**
Tampering	Integrity	Modifying data or code	Modifying a DLL on disk or DVD, or a packet as it traverses the LAN.
Repudiation	Non-repudiation	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.

Mitigate



- Address each threat
- Four ways to address threats:
  - Redesign to eliminate
  - Apply standard mitigations
    - Michael Howard’s “Implementing Threat Mitigations”
    - What have similar software packages done?
      - How has that worked out for them?
  - Invent new mitigations
    - Riskier
  - Accept vulnerability in design
    - SDL rules about what you can accept
- Address each threat

Validate



- Validate the whole TM
  - Does diagram match final code?
  - Are threats are enumerated?
  - Minimum: STRIDE per element that touches a trust boundary
  - Has test reviewed the model?
    - Tester approach often finds issues with TM, or details

- Is each threat mitigated?
  - Are mitigations done right
  - Examples are tremendously helpful here

THREAT MODELING:

FUTURE

Diverse Ecosystem of TM

- Processes and tools which work for the problem at hand
- Select one that will work for your project
  - Asset, attacker or software
  - Waterfall or agile
  - Experts or everyone
  - Firmware, boxed software, web, LoB, new devices, protocols, enterprises, etc
- Guidance from the philosophical to the prescriptive

watch this space. ☺

THANK YOU