THREAT MODELING | LAB

Continuous Security

Leverage incremental threat modeling

November 9th | 11:00am-12:30pm ET

Irene Michlin
Application Security Lead, Neo4j

Agenda

11:00 Welcome and intro
11:05 Presentation (15 mins)

11:20 Exercise 1: Breakout room (30 mins)
11:50 Readout of exercise 1 (10 mins)

12:00 Break (10 mins)

12:10 Exercise 2: Breakout room (30 mins)
12:40 Readout of exercise 2 (10 mins)

12:50 Conclusion
12:55 Questions

Ground Rules

- **Be present:** Close off emails, Slack, other unnecessary windows to keep distractions at bay :)
- **Turn on your video if possible (except during individual exercise):** Help yourself and others stay engaged!
- **Be back on time:** So we can maximize the two hours together and finish on time

Learning Objectives

By the end of this workshop, you'll:

- Learn to identify manageable chunks for your threat modelling session

Assumptions:

- You have some idea of what DFD and STRIDE are

Refresher

1. **What are we building?**

   Decompose architecture using DFDs

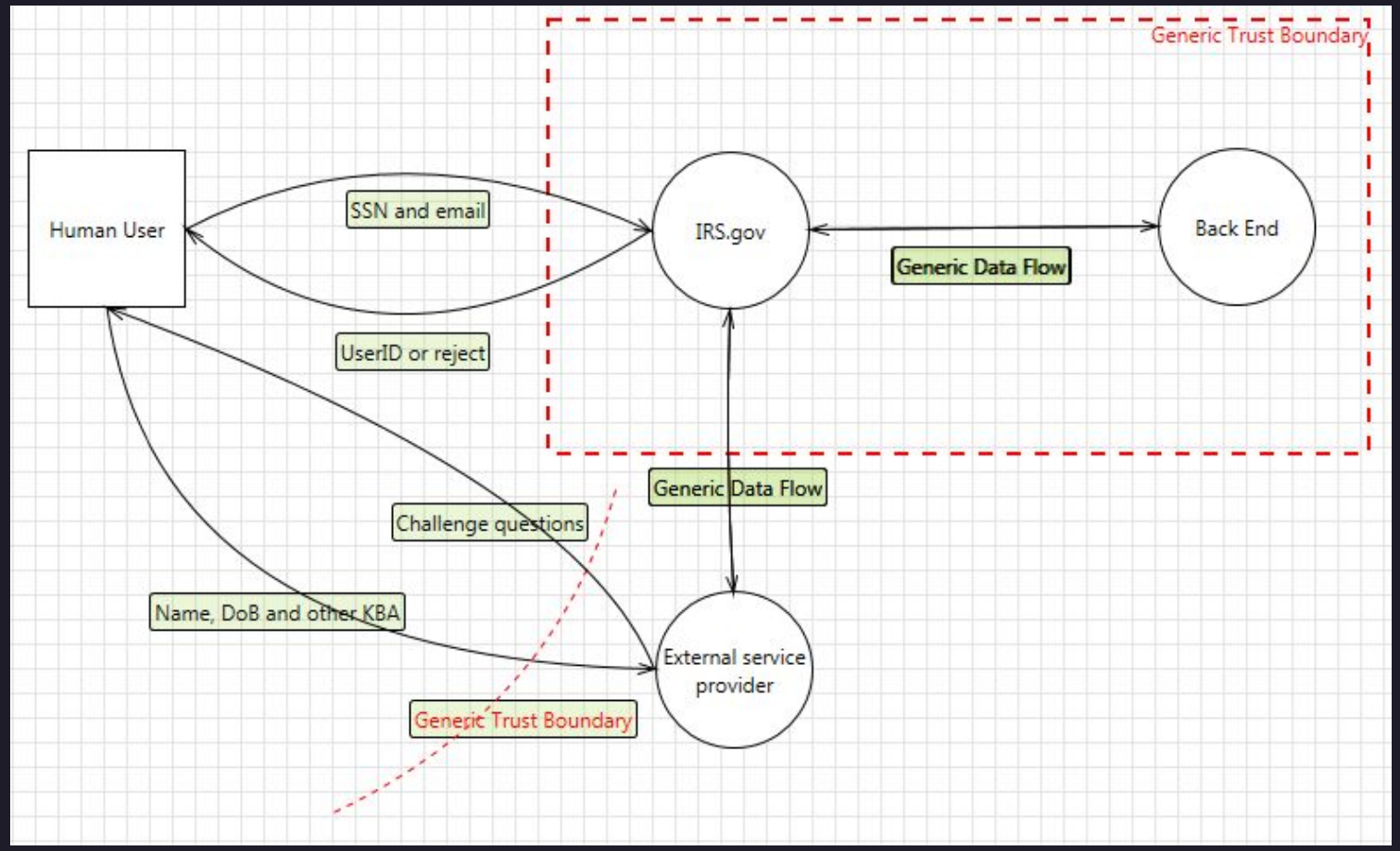
2. **What can go wrong?**

   Search for threats using STRIDE

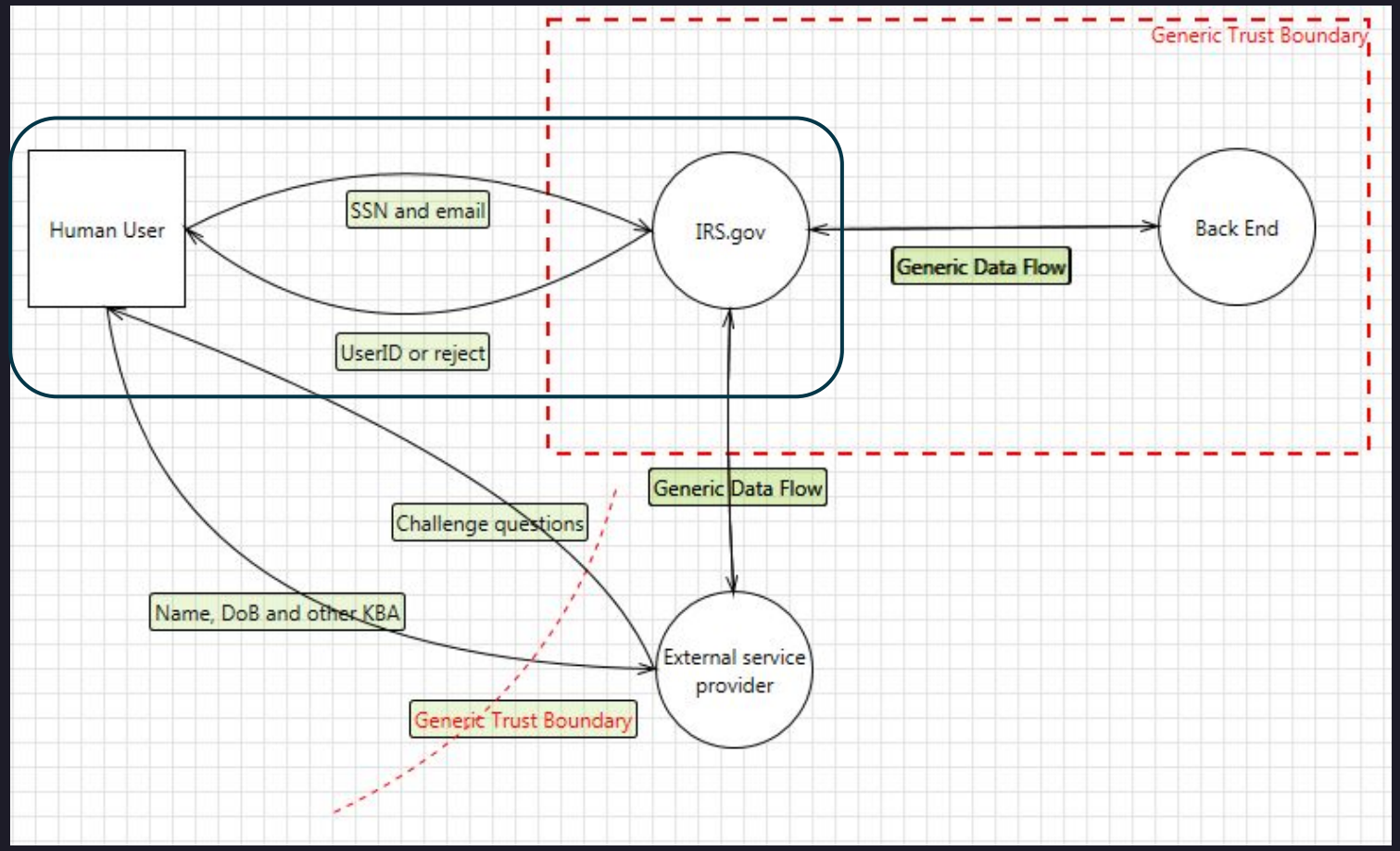
3. **What are we going to do about that?**

4. **Have we done a good enough job?**

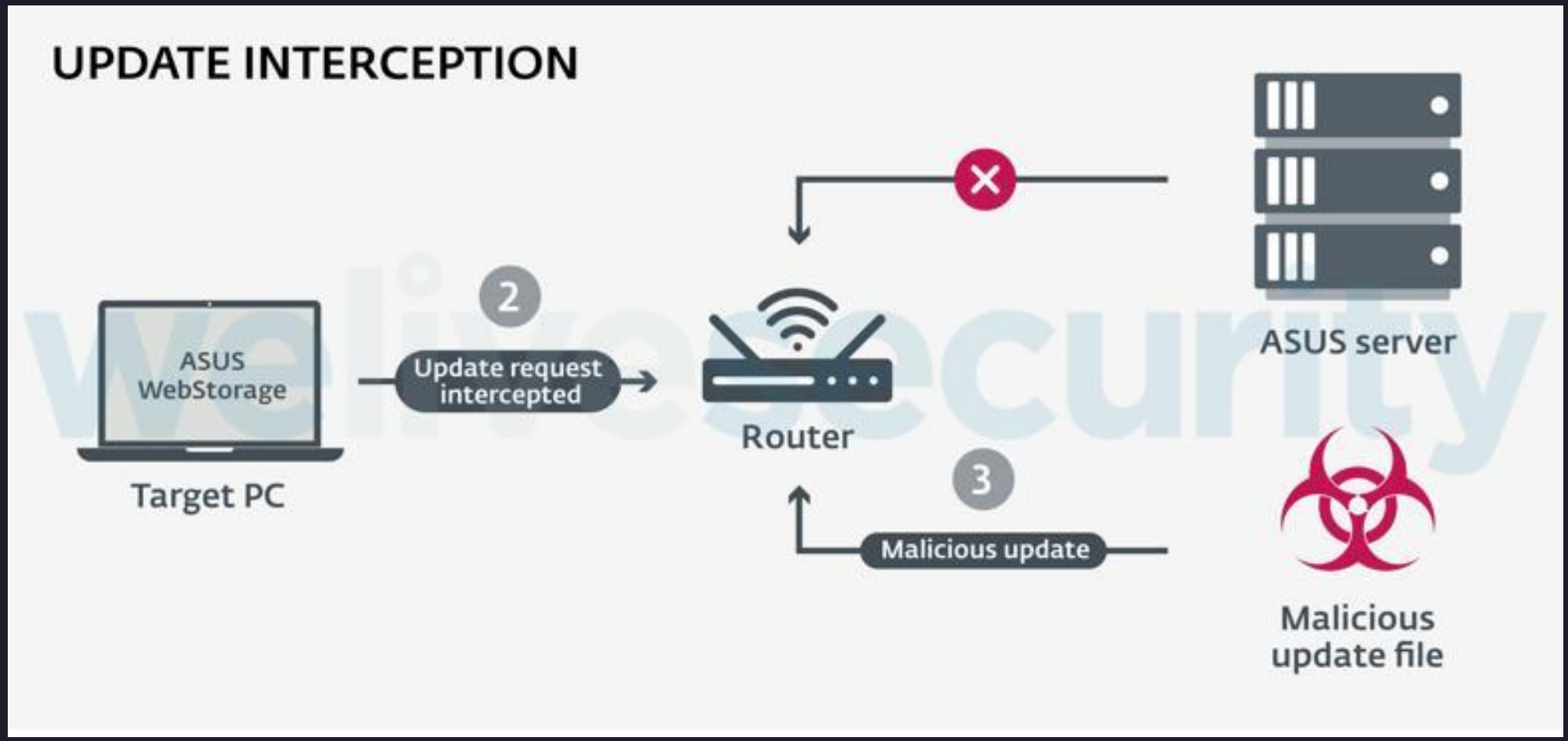
Data Flow Diagrams



Spoofing


Generic Trust Boundary
Human User
SSN and email
IRS.gov
Back End
Generic Data Flow
UserID or reject
Generic Data Flow
Challenge questions
Name, DoB and other KBA
External service provider
Generic Trust Boundary

Tampering


UPDATE INTERCEPTION
ASUS WebStorage
Target PC
2
Update request intercepted
Router
ASUS server
3
Malicious update
Malicious update file

Exercise time!

https://miro.com/welcomeonboard/RmVUME9tY0IxWTJZWURrN0FrUm9xN1d5ZnY0aIBhMHNLNnlPMTVmM0VRSnVHUTdoQVlPeDZxUXFlOWNkTG1pSXwzNDU4NzY0NTU2MDMwMzMyMDE0fDI=?share_link_id=811788684967

Conclusion

1. **Can’t get away with doing only incremental, but it’s a great entry point**

   Fits with story-based development

2. **Incremental threat modelling can fit any time-box**

   Tool 1: New and changed components and data flows, everything else is legacy blob

   Tool 2: We are not making it (legacy blob) worse

   Tool 3: Not our problem right now

3. **You can build a model of the whole system in parallel, or wait for several cycles**

4. **Don’t wait for the start of the new perfect project**

Useful links

http://michenriksen.com/blog/drawio-for-threat-modeling/

Wrap-Up

Q&A