C3 SECURITY

THREAT MODEL WORKSHOP

FAST TRACK

https://threatmodel.co.uk

C3 SECURITY

WHAT IS A THREAT MODEL?

CYBER SECURITY HYGIENE

C3 SECURITY

OBJECTIVES OF A THREAT MODEL

IDENTIFY

- potential vulnerabilities and/or threats

DESCRIBE

- counter-measures to mitigate risk

PRIORITISE

- resources to maximise system security

C3 SECURITY

OBJECTIVES OF A THREAT MODEL

DOCUMENTING RISK

C3 SECURITY

THE VALUE PROPOSITION: RISK MITIGATION

REPUTATION

- loss of customer confidence and trust; a weakened brand

OPERATIONS

- disruption of business operations

FINANCIAL

- loss of earnings, fines & restitution

GOVERNANCE & COMPLIANCE

- GDPR, Data Protection Act 2008, ISO27001 et. al.

C3 SECURITY

JUST LIKE THE FUNCTIONAL, DESIGN AND TEST SPECS, A THREAT MODEL IS A LIVING DOCUMENT — AS YOU CHANGE THE DESIGN, YOU NEED TO GO BACK AND UPDATE YOUR THREAT MODEL TO SEE IF ANY NEW THREATS HAVE ARISEN SINCE YOU STARTED.

Larry Osterman, Microsoft

C3 SECURITY

THREAT MODELLING

DOCUMENTING RISK

https://threatmodel.co.uk

C3 SECURITY

FUNDAMENTAL QUESTIONS: ASK YOURSELF

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?

Adapted from "Application Threat Modelling" by **OWASP**
https://owasp.org/www-community/Application_Threat_Modeling

C3 SECURITY

THREAT MODELLING: A PROCESS

IDENTIFY

- Using **DATA FLOW DIAGRAMS**

CLASSIFY

- Using **S.T.R.I.D.E** and **ATTACK TREES**

QUANTIFY

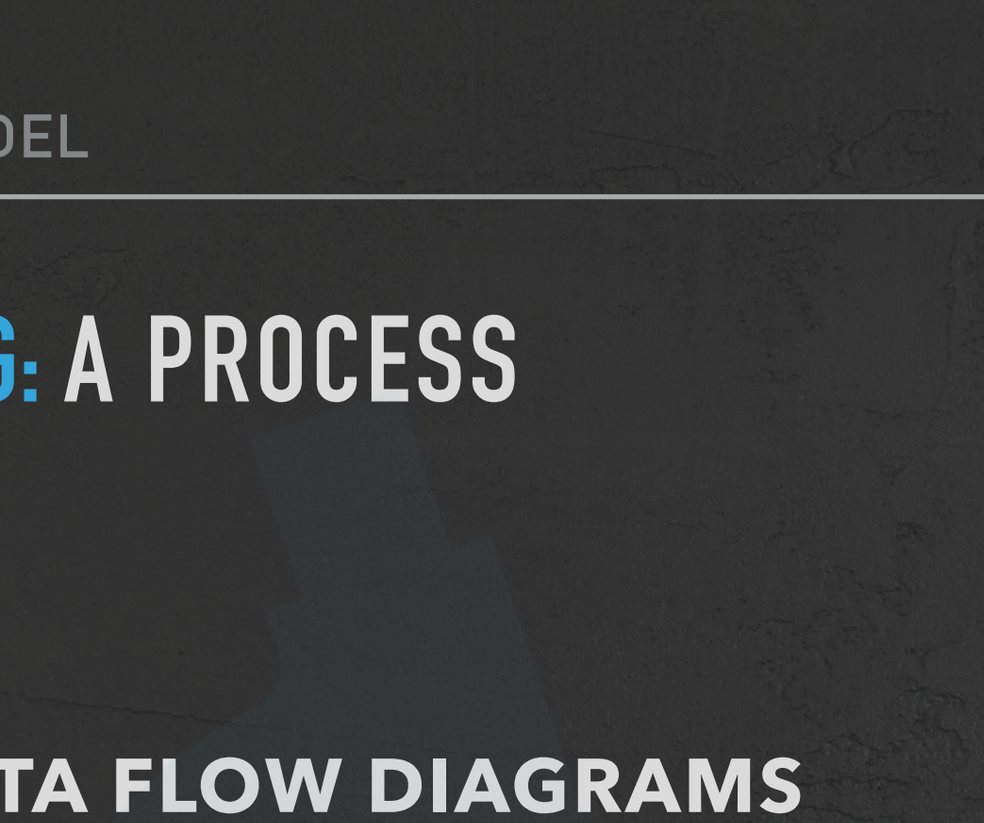
- Using **D.R.E.A.D** methodology

C3 SECURITY

THREAT MODELLING: A PROCESS

IDENTIFY

- Using **DATA FLOW DIAGRAMS**



C3 SECURITY

CLOUD
DATA BUCKET

1. STORE
DATA

IOT
DEVICE

TRUST BOUNDARY
#1

3. FETCH DATA

TRUST BOUNDARY
#2

2. REQUEST
DATA

API
GATEWAY

MOBILE
CLIENT

4. RETURN
DATA

C3 SECURITY

THREAT MODELLING: A PROCESS

IDENTIFY

- Using **DATA FLOW DIAGRAMS**

CLASSIFY

- Using **S.T.R.I.D.E** and **ATTACK TREES**

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

- **S** POOFING
- **T** AMPERING
- **R** EPUDIATION
- **I** NFORMATION (disclosure)
- **D** ENIAL (of service)
- **E** LEVATION (of privilege)

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

- **S** POOFING

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

SPOOFING

- FRAUDULENT OR MISLEADING DATA
- IMPERSONATING LEGITIMATE USERS
- PRETENDING TO BE SOMETHING IT ISN'T

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

- **S** POOFING
- **T** AMPERING

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

TAMPERING

- UNAUTHORISED CHANGES TO DATA
- MAN-IN-THE-MIDDLE (MITM) ATTACKS
- INTERFERING WITH DATA INTEGRITY

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

- **S** POOFING
- **T** AMPERING
- **R** EPUDIATION

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

REPUDIATION

- IS THERE AN AUDIT TRAIL?
- ATTACKER HIDING THEIR ACTIVITY
- PREVENTED LOGGING OF USER ACTIONS

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

- **S** POOFING
- **T** AMPERING
- **R** EPUDIATION
- **I** NFORMATION (disclosure)

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

INFORMATION DISCLOSURE

- ✦ DATA TRANSMITTED UNENCRYPTED
- ✦ LEAKING OF PERSONAL DATA (PII)
- ✦ INADEQUATE ACCESS CONTROL LIST (ACL)

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

- **S** POOFING
- **T** AMPERING
- **R** EPUDIATION
- **I** NFORMATION (disclosure)
- **D** ENIAL (of service)

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

DENIAL OF SERVICE (DOS)

- INACCESSIBLE PRODUCTS OR SERVICES
- RESOURCE EXHAUSTION
- REDUCED PERFORMANCE

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

- **S** POOFING
- **T** AMPERING
- **R** EPUDIATION
- **I** NFORMATION (disclosure)
- **D** ENIAL (of service)
- **E** LEVATION (of privilege)

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

ELEVATION OF PRIVILEGE

- BUGS, EXPLOITS AND MISCONFIGURATION INCREASING A USER'S ACCESS LEVEL
- USERS BEING ABLE TO ACCESS SERVICES OR RESOURCES WHICH THEY SHOULDN'T

C3 SECURITY

THE S.T.R.I.D.E. METHODOLOGY

- **S** POOFING
- **T** AMPERING
- **R** EPUDIATION
- **I** NFORMATION (disclosure)
- **D** ENIAL (of service)
- **E** LEVATION (of privilege)

C3 SECURITY

THREAT MODELLING: A PROCESS

IDENTIFY

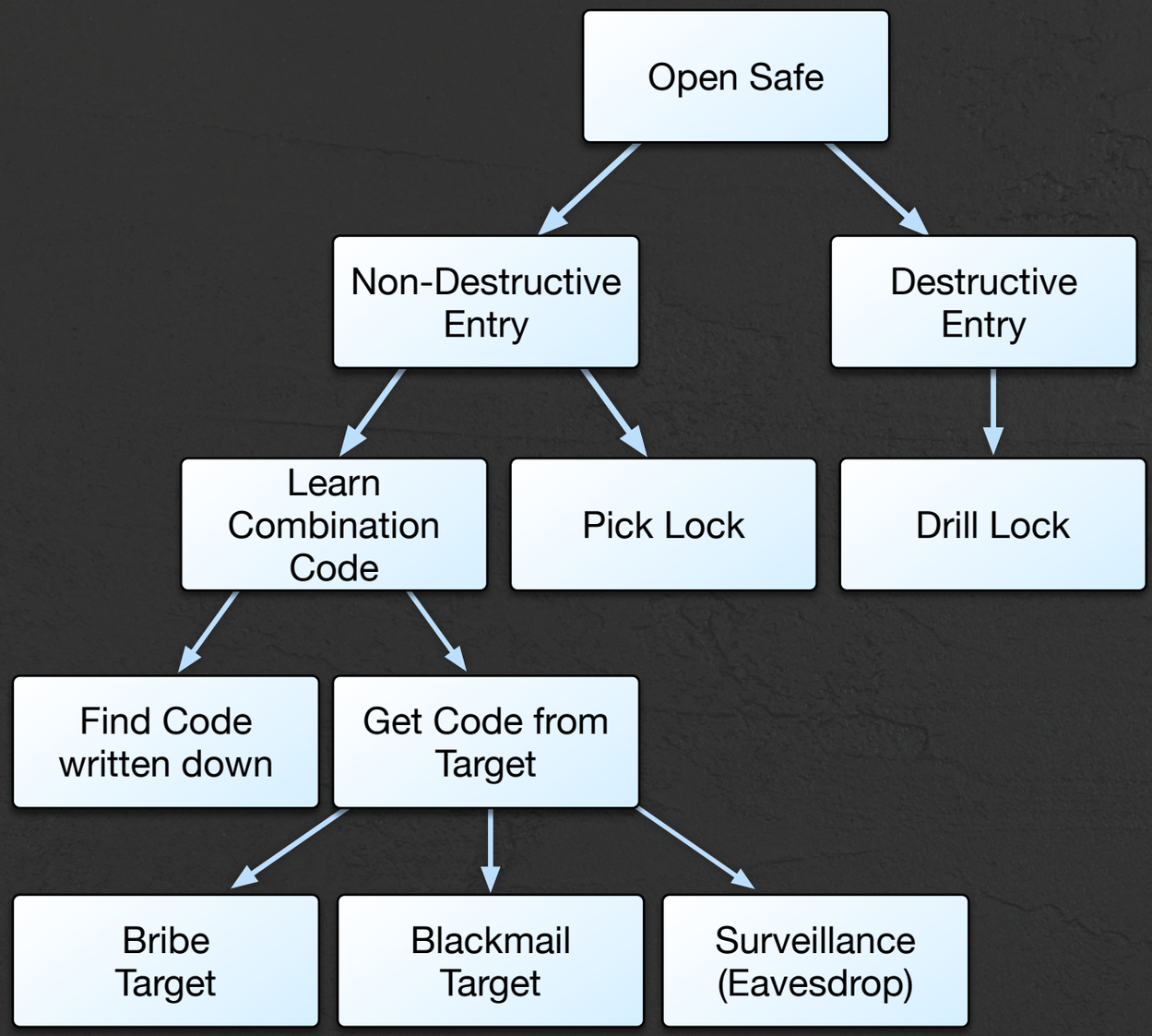
- Using **DATA FLOW DIAGRAMS**

CLASSIFY

- Using **S.T.R.I.D.E** and **ATTACK TREES**

C3 SECURITY

THE ATTACK TREE METHODOLOGY



Adapted from “Attack Trees” by **Bruce Schneier**, Dr. Dobb's Journal, 1999

C3 SECURITY

THREAT MODELLING: A PROCESS

IDENTIFY

- Using **DATA FLOW DIAGRAMS**

CLASSIFY

- Using **S.T.R.I.D.E** and **ATTACK TREES**

QUANTIFY

- Using **D.R.E.A.D** methodology

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

- **D AMAGE**
- **R EPRODUCIBILITY**
- **E XPLOITABILITY**
- **A FFECTED** (users)
- **D ISCOVERABILITY**

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

D AMAGE

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

DAMAGE

- HOW BAD WOULD AN ATTACK BE?
- FROM THE BUSINESS AND SERVICE PERSPECTIVES

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

- **D AMAGE**
- **R EPRODUCIBILITY**

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

REPRODUCIBILITY

- HOW EASY IS IT TO REPRODUCE?
- IS IT PREDICTABLE OR UNPREDICTABLE?
- ARE THERE OTHER FACTORS REQUIRED?

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

- **D** AMAGE
- **R** EPRODUCIBILITY
- **E** XPLOITABILITY

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

EXPLOITABILITY

- ✦ HOW EASY IS IT TO EXPLOIT?
- ✦ IS EXPLOITING SIMPLE OR COMPLEX?
- ✦ REQUIRES MULTIPLE VULNERABILITIES?

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

- **D AMAGE**
- **R EPRODUCIBILITY**
- **E XPLOITABILITY**
- **A FFECTED** (users)

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

AFFECTED USERS

- HOW MANY USERS WILL IT IMPACT?
- DOES IT AFFECT ONLY SERVICE USERS?

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

- **D AMAGE**
- **R EPRODUCIBILITY**
- **E XPLOITABILITY**
- **A FFECTED** (users)
- **D ISCOVERABILITY**

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

DISCOVERABILITY

- HOW EASY IS IT TO DISCOVER THE VULNERABILITY?
- EXPOSED CONFIGURATION INFORMATION

C3 SECURITY

THE D.R.E.A.D. RISK ASSESSMENT

- **D AMAGE**
- **R EPRODUCIBILITY**
- **E XPLOITABILITY**
- **A FFECTED** (users)
- **D ISCOVERABILITY**

C3 SECURITY

IT IS NEVER TOO LATE AND IT IS NEVER TOO EARLY TO DOCUMENT RISK. THE BEST TIME TO THREAT MODEL IS NOW!

Anonymous