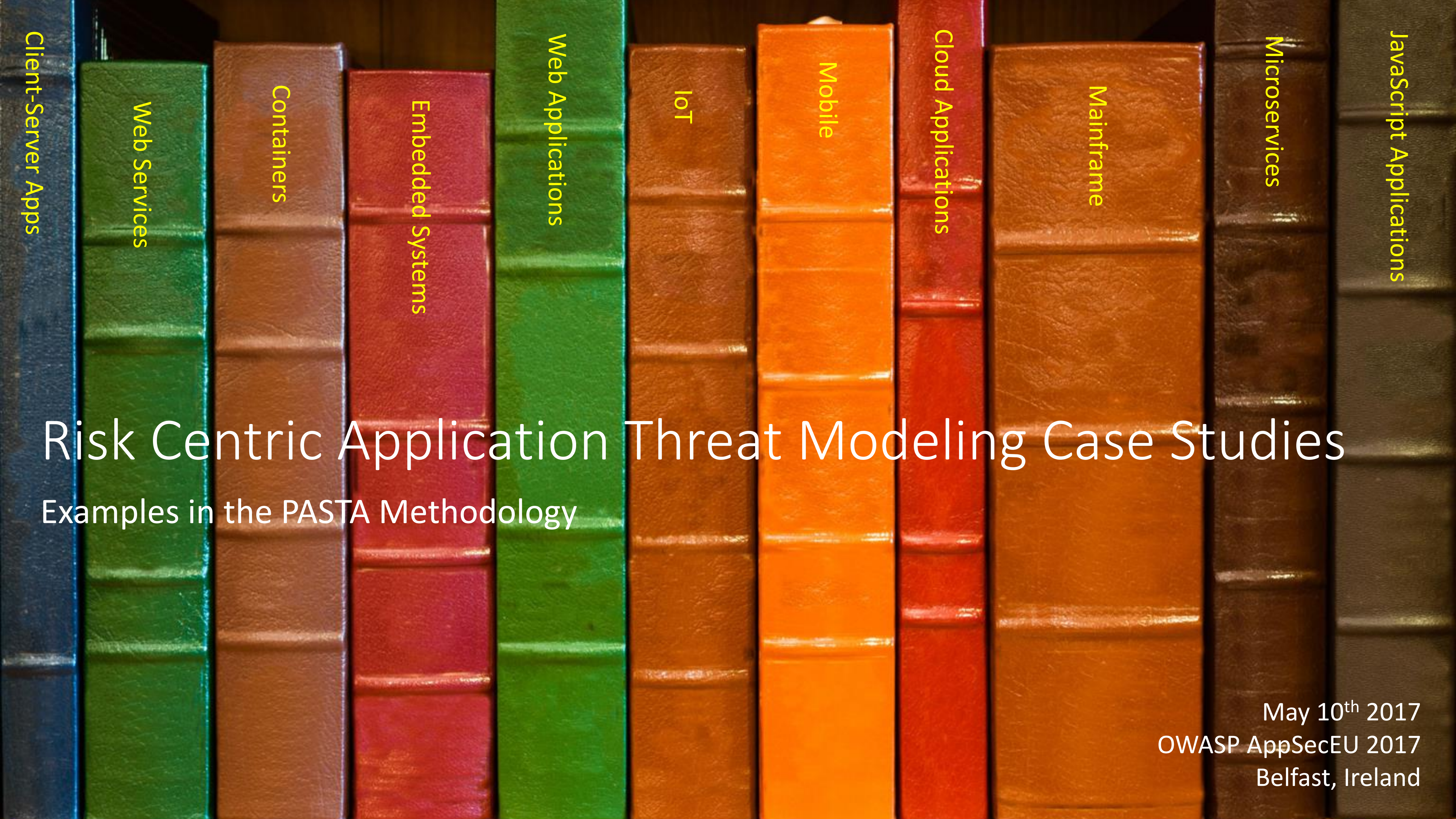
OWASP
AppSec EU
Belfast
8-12 May, 2017

Threat Modeling w/ PASTA

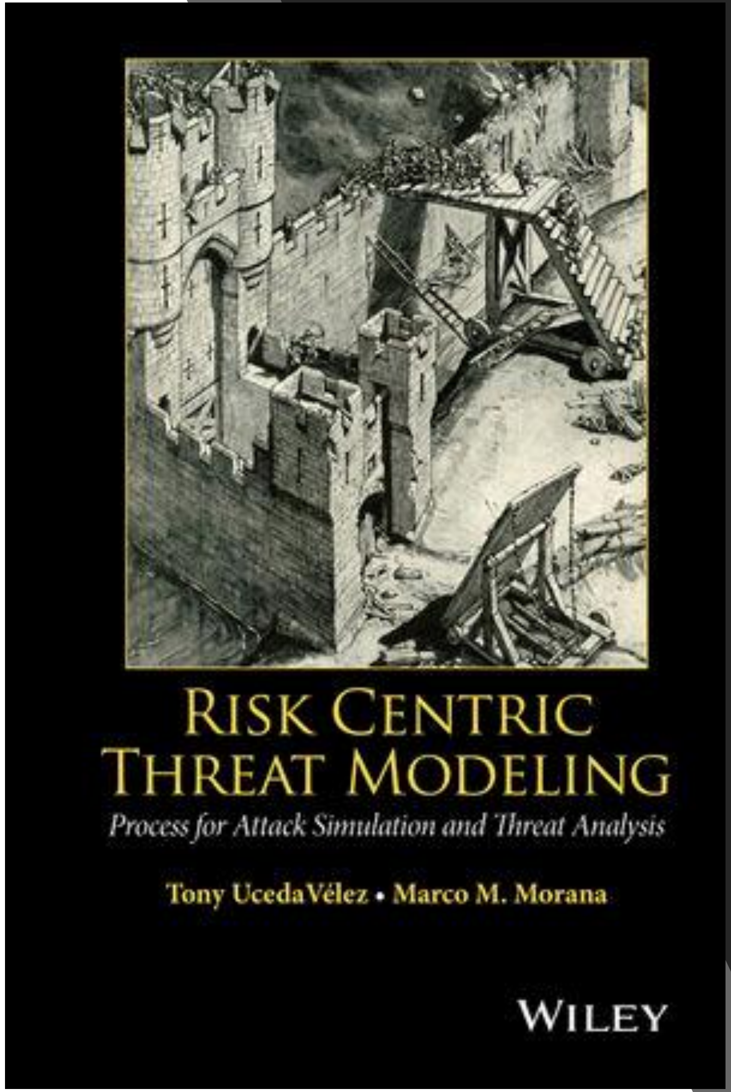
Risk Centric Threat Modeling Case Studies



Risk Centric Application Threat Modeling Case Studies

Examples in the PASTA Methodology

May 10th 2017
OWASP AppSecEU 2017
Belfast, Ireland



RISK CENTRIC
THREAT MODELING
Process for Attack Simulation and Threat Analysis
Tony UcedaVélez • Marco M. Morana
WILEY

Speaker Bio

- Tony UcedaVélez (“Tony UV”)
  - CEO, VerSprite (www.versprite.com) – Global Security Consulting Firm
  - Chapter Leader – OWASP Atlanta (past 10 years)
  - Author, “Risk Centric Threat Modeling – Process for Attack Simulation & Threat Analysis”, Wiley June 2015
  - U.S Federal Government, GE, SunTrust Banks, UBS, Symantec, Dell-Secureworks, Equifax
  - @t0nyuv (Twitter)
  - tonyuv@versprite.com

- Model of Threats
- Threats become realized via Attacks
- Threat **Intel** fuels knowledge on styles of attack by adversaries
- Threat **data** may represent lessons learned from prior battles/ attacks
  - May reveal new attack patterns
- Model of threats provides war leaders on a ‘model’ of threats to consider

Dissecting “Threat Modeling”

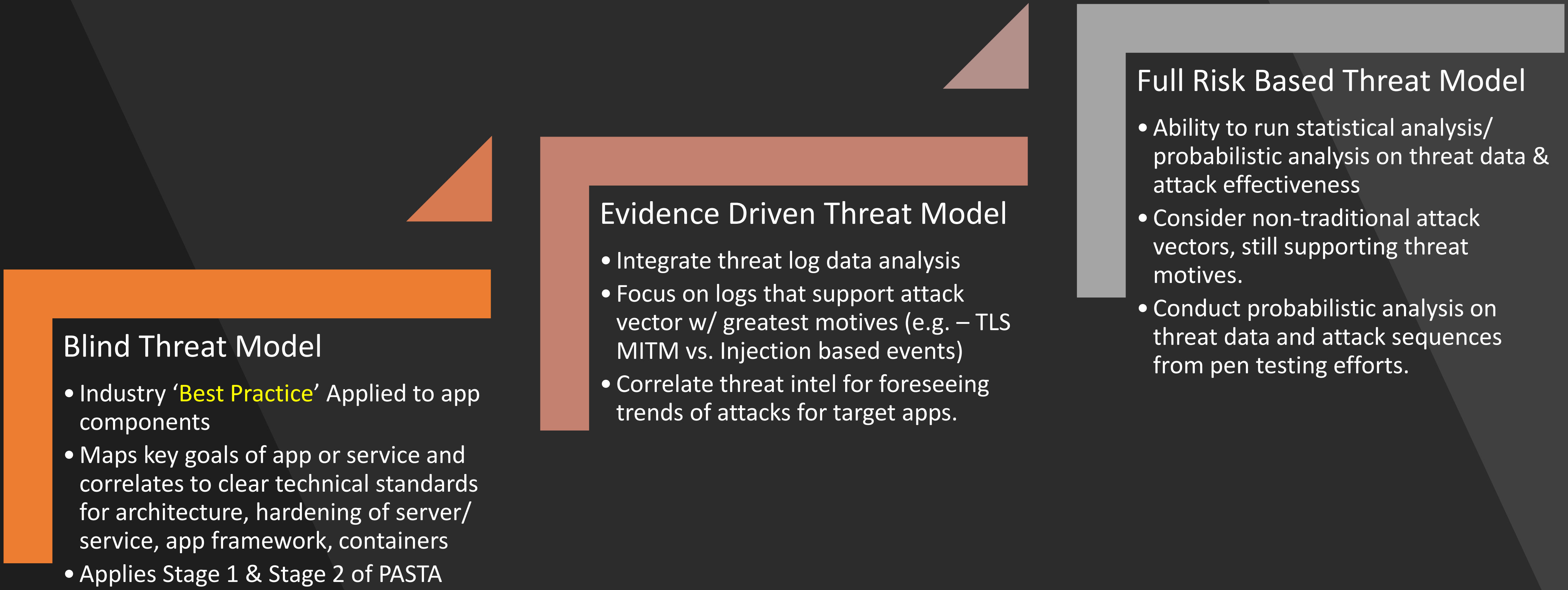
PASTA (Risk Centric) Objectives

- ❑Risk centric has the objective of mitigating what matters
- ❑Evidence based threat modeling
  - ❑Harvest **threat intel** to support **threat motives**
  - ❑Leverage **threat data** to support prior **threat patterns**
- ❑Risk based approach focuses a lot on probability of attack(s), threat likelihood, inherent risk, impact of compromise
- ❑ ‘If there is little to no impact, why spend time/ money on security?’
- ❑ Collaborative
- ❑ Prioritization model should define when and what apps to threat model

Taxonomy of Terms

- **Asset.** An asset is a resource of value. It varies by perspective. To your business, an asset might be the availability of information, or the information itself, such as customer data. It might be intangible, such as your company's reputation.
- **Threat.** A threat is an undesired event. A potential occurrence, often best described as an effect that might damage or compromise an asset or objective.
- **Vulnerability.** A vulnerability is a software/ firmware code imperfection at the system, network, or framework level that makes an exploit possible.
- **Attack (or exploit).** An attack is an action taken that utilizes one or more vulnerabilities to realize a threat.
- **Countermeasure.** Countermeasures address vulnerabilities to reduce the probability of attacks or the impacts of threats. They do not directly address threats; instead, they address the factors that define the threats.
- **Use Case.** Functional, as designed function of an application.
- **Abuse Case.** Deliberate abuse of use case in order to produce unintended results
- **Attack Vector.** Point & channel for which attacks traverse over (card reader, form fields, network proxy)
- **Attack Surface.** Logical area exposed for threats & underlying attack patterns
- **Actor.** Legit or adverse caller of use or abuse cases.
- **Impact.** Negative value sustained by successful attack(s)
- **Attack Tree.** Diagram of relationship amongst asset-actor-use case-abuse case-vuln-exploit-countermeasure

How to Get Started w/ PASTA :: 3 Tiers



Blind Threat Model

- Industry ‘Best Practice’ Applied to app components
- Maps key goals of app or service and correlates to clear technical standards for architecture, hardening of server/ service, app framework, containers
- Applies Stage 1 & Stage 2 of PASTA

Evidence Driven Threat Model

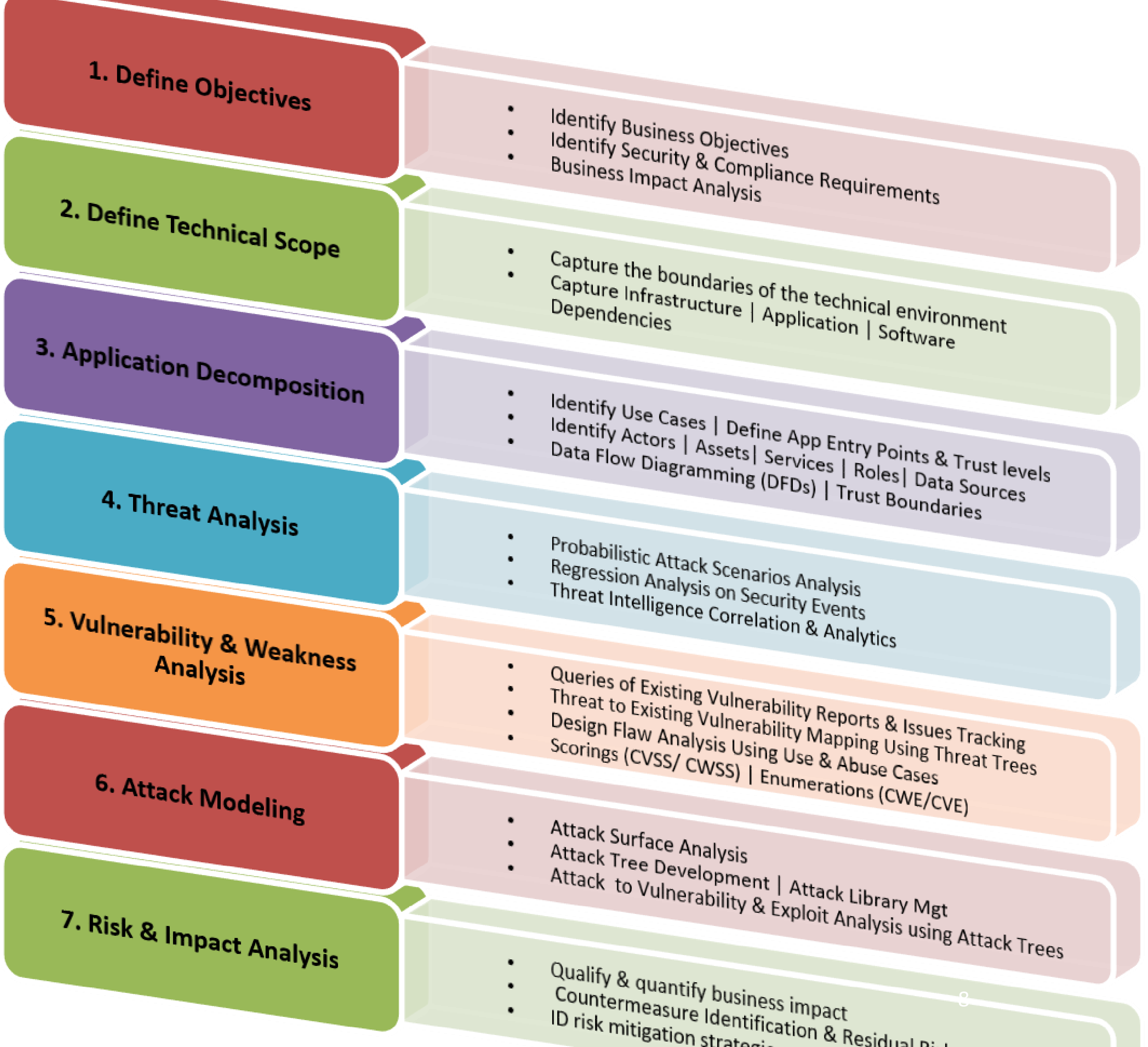
- Integrate threat log data analysis
- Focus on logs that support attack vector w/ greatest motives (e.g. – TLS MITM vs. Injection based events)
- Correlate threat intel for foreseeing trends of attacks for target apps.

Full Risk Based Threat Model

- Ability to run statistical analysis/ probabilistic analysis on threat data & attack effectiveness
- Consider non-traditional attack vectors, still supporting threat motives.
- Conduct probabilistic analysis on threat data and attack sequences from pen testing efforts.

Process for Attack Simulation & Threat Analysis

- Stage I sets tone of importance around **use cases**
- Stage II defines **technical scope** of app components
- Stage III **maps** what's important to what's in scope (**DFDs**)
- Stage IV correlates relevant **threat patterns**
- Stage V & VI – "**proof**" stages; prove viability
- Stage VII – Rationale for **countermeasure development** based upon **residual risk**



1. Define Objectives

- Identify Business Objectives
- Identify Security & Compliance Requirements
- Business Impact Analysis

2. Define Technical Scope

- Capture the boundaries of the technical environment
- Capture Infrastructure | Application | Software Dependencies

3. Application Decomposition

- Identify Use Cases | Define App Entry Points & Trust levels
- Identify Actors | Assets| Services | Roles| Data Sources
- Data Flow Diagramming (DFDs) | Trust Boundaries

4. Threat Analysis

- Probabilistic Attack Scenarios Analysis
- Regression Analysis on Security Events
- Threat Intelligence Correlation & Analytics

5. Vulnerability & Weakness Analysis

- Queries of Existing Vulnerability Reports & Issues Tracking
- Threat to Existing Vulnerability Mapping Using Threat Trees
- Design Flaw Analysis Using Use & Abuse Cases
- Scorings (CVSS/ CWSS) | Enumerations (CWE/CVE)

6. Attack Modeling

- Attack Surface Analysis
- Attack Tree Development | Attack Library Mgt
- Attack to Vulnerability & Exploit Analysis using Attack Trees

7. Risk & Impact Analysis

- Qualify & quantify business impact
- Countermeasure Identification & Residual Ri
- ID risk mitigation strategi

Measuring Residual Risk

$$\text{Residual Risk} = \frac{\text{Vuln}_{(p1)}*\text{Attack}_{(p2)}*\text{Impact}}{\text{Countermeasures}}$$

- Remediate in commensuration to identified Risk
- Risk !=t * v * i
- Risk! = t * v * i * p
- [(tp * vp)/c] * i = Rrisk
- Attack simulation enhances (p) probability coefficients
- Considers both inherent countermeasures & those to be developed
- Focused on minimizing risks to mobile based use cases that truly impact business

Risk Triangle

Probabilistic Analysis Substantiates Threat Assertions

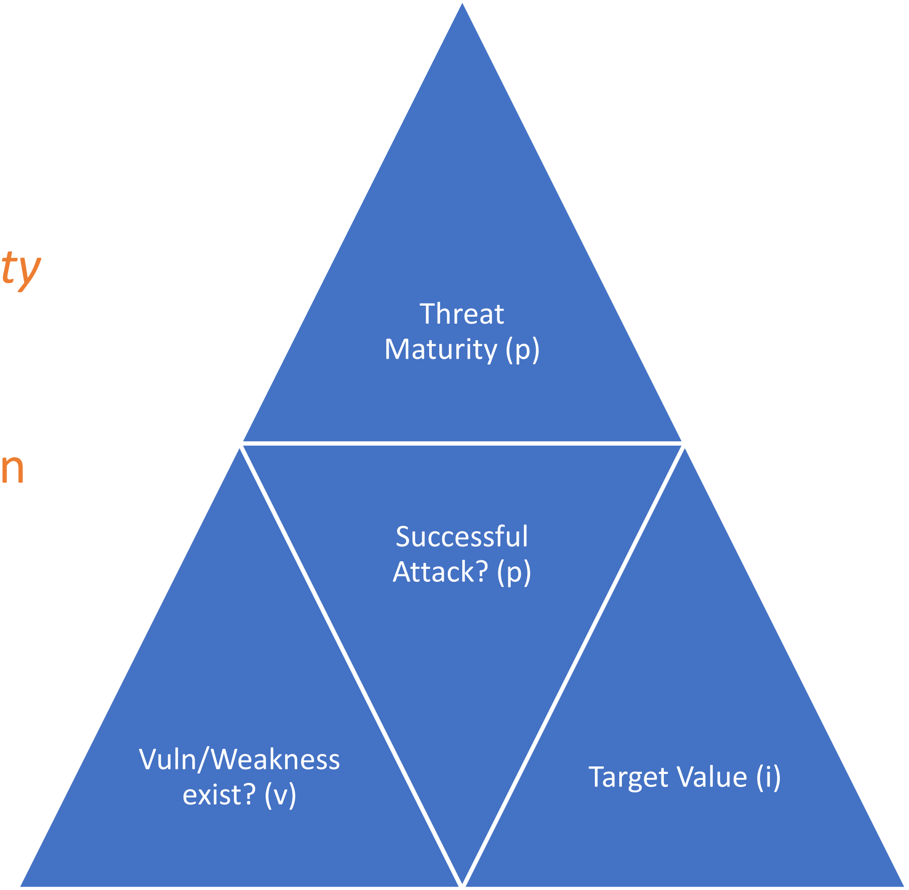
- ❑ Can be a binary exercise for threat viability
- ❑ WALK, RUN versions of model suggest weighted probability bands for *maturity* of threats, attacks, vulns, etc.
- ❑ Pen testing validates attack feasibility
  - ▪ Requires large data to do regression analysis OR
  - ▪ Use probabilistic bands

  P < 25%

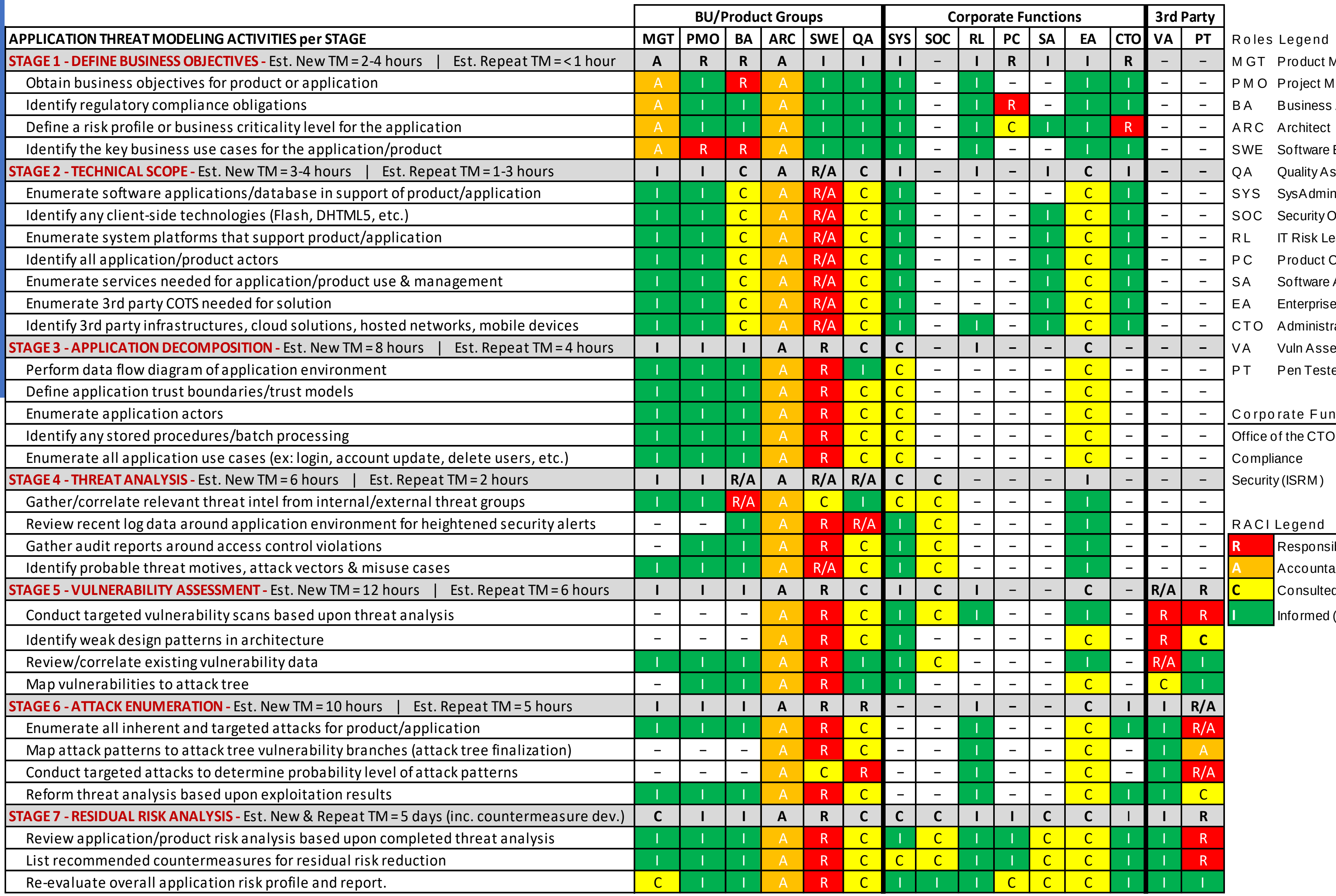
  25% < P < 50%

  50% < P < 75%

  P > 75%



RACI & PASTA



	BU/Product Groups						Corporate Functions							3rd Party	
APPLICATION THREAT MODELING ACTIVITIES per STAGE	**MGT**	**PMO**	**BA**	**ARC**	**SWE**	**QA**	**SYS**	**SOC**	**RL**	**PC**	**SA**	**EA**	**CTO**	**VA**	**PT**
STAGE 1 - DEFINE BUSINESS OBJECTIVES - Est. New TM = 2-4 hours | Est. Repeat TM = < 1 hour	**A**	**R**	**R**	**A**	**I**	**I**	**I**	**–**	**I**	**R**	**I**	**I**	**R**	**–**	**–**
Obtain business objectives for product or application	A	I	R	A	I	I	I	–	I	–	–	I	I	–	–
Identify regulatory compliance obligations	A	I	I	A	I	I	I	–	I	R	–	I	I	–	–
Define a risk profile or business criticality level for the application	A	I	I	A	I	I	I	–	I	C	I	I	R	–	–
Identify the key business use cases for the application/product	A	R	R	A	I	I	I	–	I	–	–	I	I	–	–
STAGE 2 - TECHNICAL SCOPE - Est. New TM = 3-4 hours | Est. Repeat TM = 1-3 hours	**I**	**I**	**C**	**A**	**R/A**	**C**	**I**	**–**	**I**	**–**	**I**	**C**	**I**	**–**	**–**
Enumerate software applications/database in support of product/application	I	I	C	A	R/A	C	I	–	–	–	–	C	I	–	–
Identify any client-side technologies (Flash, DHTML5, etc.)	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Enumerate system platforms that support product/application	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Identify all application/product actors	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Enumerate services needed for application/product use & management	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Enumerate 3rd party COTS needed for solution	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Identify 3rd party infrastructures, cloud solutions, hosted networks, mobile devices	I	I	C	A	R/A	C	I	–	I	–	I	C	I	–	–
STAGE 3 - APPLICATION DECOMPOSITION - Est. New TM = 8 hours | Est. Repeat TM = 4 hours	**I**	**I**	**I**	**A**	**R**	**C**	**C**	**–**	**I**	**–**	**–**	**C**	**–**	**–**	**–**
Perform data flow diagram of application environment	I	I	I	A	R	I	C	–	–	–	–	C	–	–	–
Define application trust boundaries/trust models	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
Enumerate application actors	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
Identify any stored procedures/batch processing	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
Enumerate all application use cases (ex: login, account update, delete users, etc.)	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
STAGE 4 - THREAT ANALYSIS - Est. New TM = 6 hours | Est. Repeat TM = 2 hours	**I**	**I**	**R/A**	**A**	**R/A**	**R/A**	**C**	**C**	**–**	**–**	**–**	**I**	**–**	**–**	**–**
Gather/correlate relevant threat intel from internal/external threat groups	I	I	R/A	A	C	I	C	C	–	–	–	I	–	–	–
Review recent log data around application environment for heightened security alerts	–	–	I	A	R	R/A	I	C	–	–	–	I	–	–	–
Gather audit reports around access control violations	–	I	I	A	R	C	I	C	–	–	–	I	–	–	–
Identify probable threat motives, attack vectors & misuse cases	I	I	I	A	R/A	C	I	C	–	–	–	I	–	–	–
STAGE 5 - VULNERABILITY ASSESSMENT - Est. New TM = 12 hours | Est. Repeat TM = 6 hours	**I**	**I**	**I**	**A**	**R**	**C**	**I**	**C**	**I**	**–**	**–**	**C**	**–**	**R/A**	**R**
Conduct targeted vulnerability scans based upon threat analysis	–	–	–	A	R	C	I	C	I	–	–	I	–	R	R
Identify weak design patterns in architecture	–	–	–	A	R	C	I	–	–	–	–	C	–	R	C
Review/correlate existing vulnerability data	I	I	I	A	R	I	I	C	–	–	–	I	–	R/A	I
Map vulnerabilities to attack tree	–	I	I	A	R	I	I	–	–	–	–	C	–	C	I
STAGE 6 - ATTACK ENUMERATION - Est. New TM = 10 hours | Est. Repeat TM = 5 hours	**I**	**I**	**I**	**A**	**R**	**R**	**–**	**–**	**I**	**–**	**–**	**C**	**I**	**I**	**R/A**
Enumerate all inherent and targeted attacks for product/application	I	I	I	A	R	C	–	–	I	–	–	C	I	I	R/A
Map attack patterns to attack tree vulnerability branches (attack tree finalization)	–	–	–	A	R	C	–	–	I	–	–	C	–	I	A
Conduct targeted attacks to determine probability level of attack patterns	–	–	–	A	C	R	–	–	I	–	–	C	–	I	R/A
Reform threat analysis based upon exploitation results	I	I	I	A	R	C	–	–	I	–	–	C	I	I	C
STAGE 7 - RESIDUAL RISK ANALYSIS - Est. New & Repeat TM = 5 days (inc. countermeasure dev.)	**C**	**I**	**I**	**A**	**R**	**C**	**C**	**C**	**I**	**I**	**C**	**C**	I	**I**	**R**
Review application/product risk analysis based upon completed threat analysis	I	I	I	A	R	C	I	C	I	I	C	C	I	I	R
List recommended countermeasures for residual risk reduction	I	I	I	A	R	C	C	C	I	I	C	C	I	I	R
Re-evaluate overall application risk profile and report.	C	I	I	A	R	C	I	I	I	C	C	C	I	I	I

Roles Legend

MGT	Product M
PMO	Project M
BA	Business
ARC	Architect
SWE	Software E
QA	Quality As
SYS	SysAdmin
SOC	Security O
RL	IT Risk Le
PC	Product C
SA	Software A
EA	Enterprise
CTO	Administra
VA	Vuln Asse
PT	Pen Teste

Corporate Fun

Office of the CTO

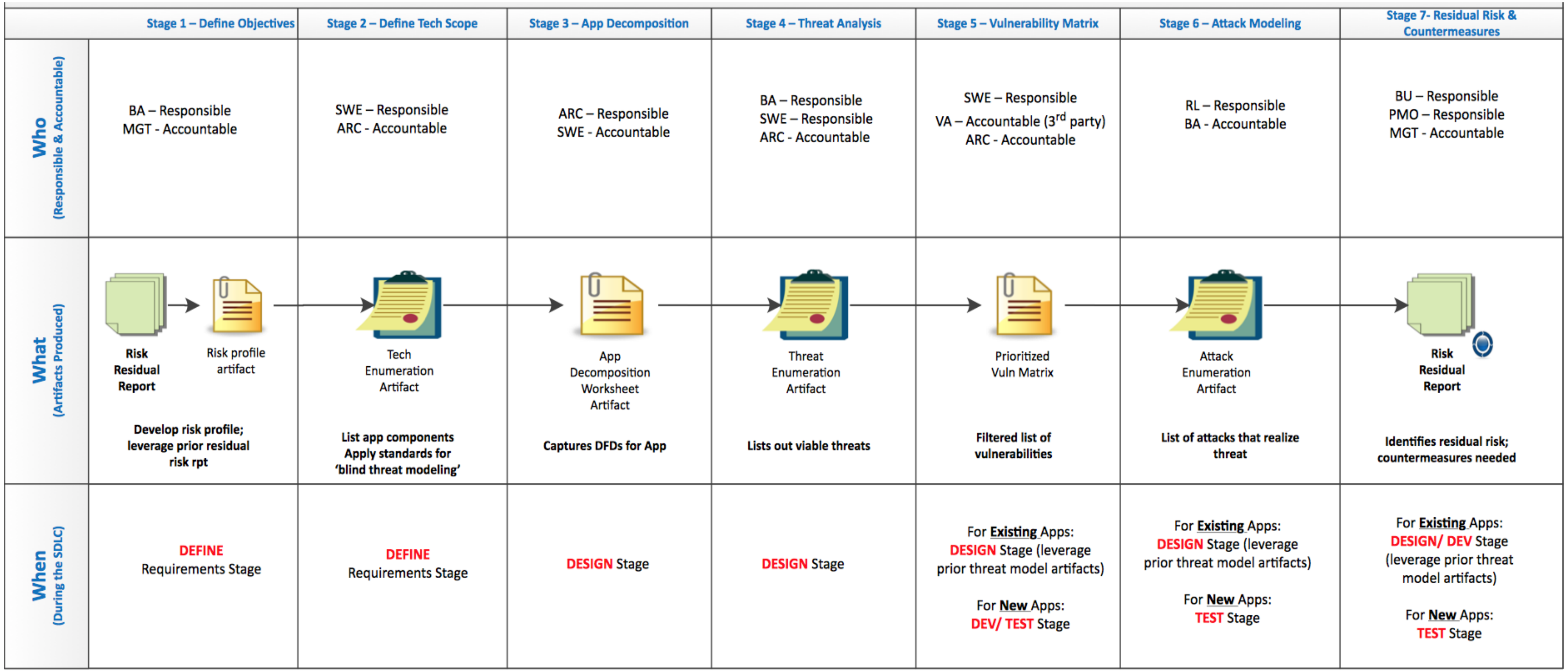
Compliance

Security (ISRM)

RACI Legend

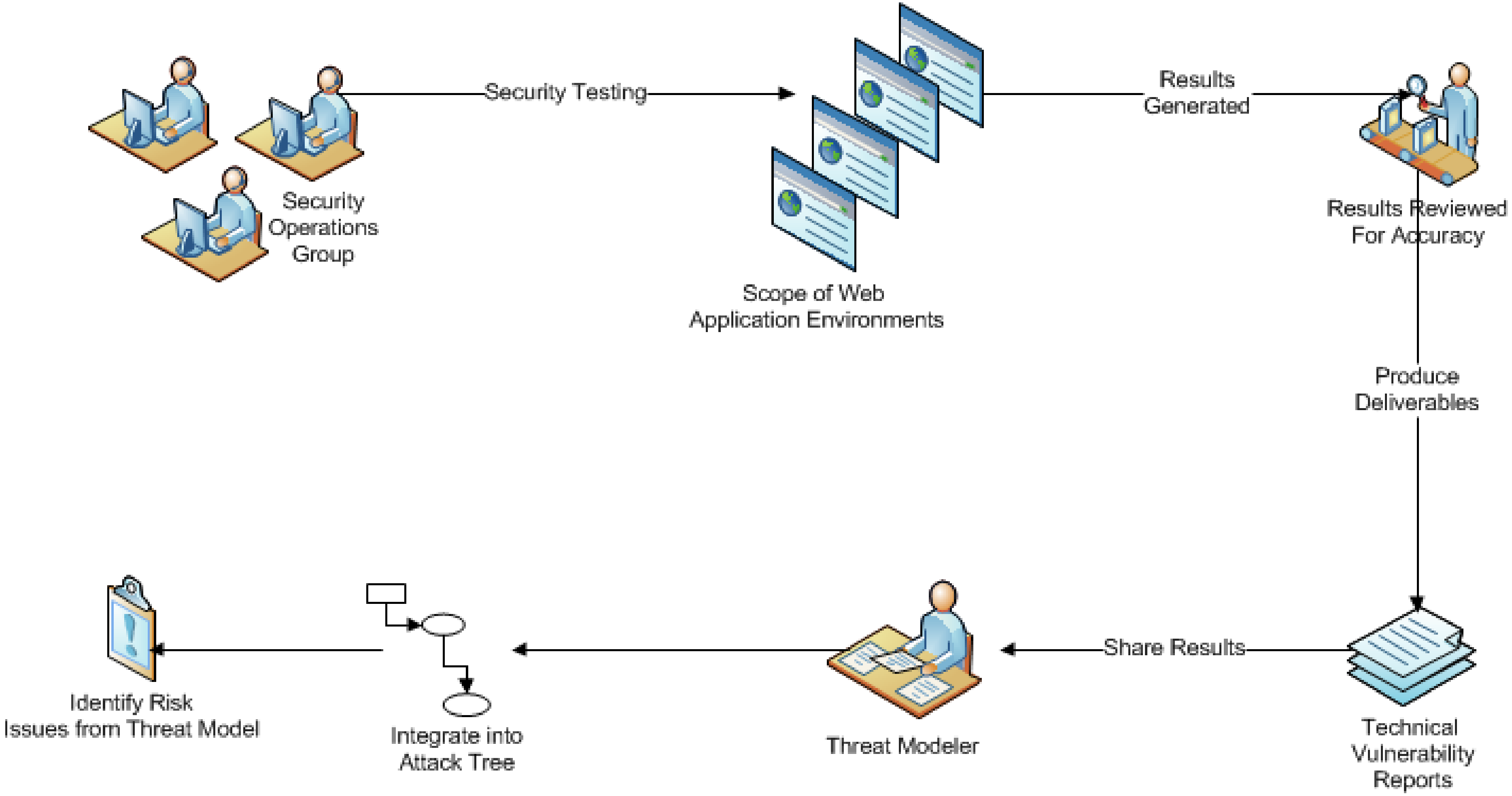
R	Responsi
A	Accounta
C	Consulted
I	Informed (

PASTA to SDLC Activity Mapping



	Stage 1 – Define Objectives	Stage 2 – Define Tech Scope	Stage 3 – App Decomposition	Stage 4 – Threat Analysis	Stage 5 – Vulnerability Matrix	Stage 6 – Attack Modeling	Stage 7- Residual Risk & Countermeasures
Who (Responsible & Accountable)	BA – Responsible MGT - Accountable	SWE – Responsible ARC - Accountable	ARC – Responsible SWE - Accountable	BA – Responsible SWE – Responsible ARC - Accountable	SWE – Responsible VA – Accountable (3rd party) ARC - Accountable	RL – Responsible BA - Accountable	BU – Responsible PMO – Responsible MGT - Accountable
What (Artifacts Produced)	**Risk Residual Report** Risk profile artifact **Develop risk profile; leverage prior residual risk rpt**	Tech Enumeration Artifact **List app components Apply standards for 'blind threat modeling'**	App Decomposition Worksheet Artifact **Captures DFDs for App**	Threat Enumeration Artifact **Lists out viable threats**	Prioritized Vuln Matrix **Filtered list of vulnerabilities**	Attack Enumeration Artifact **List of attacks that realize threat**	**Risk Residual Report** **Identifies residual risk; countermeasures needed**
When (During the SDLC)	DEFINE Requirements Stage	DEFINE Requirements Stage	DESIGN Stage	DESIGN Stage	For **Existing** Apps: DESIGN Stage (leverage prior threat model artifacts) For **New** Apps: DEV/ TEST Stage	For **Existing** Apps: DESIGN Stage (leverage prior threat model artifacts) For **New** Apps: TEST Stage	For **Existing** Apps: DESIGN/ DEV Stage (leverage prior threat model artifacts) For **New** Apps: TEST Stage

PASTA & Collaboration :: Integrative Process

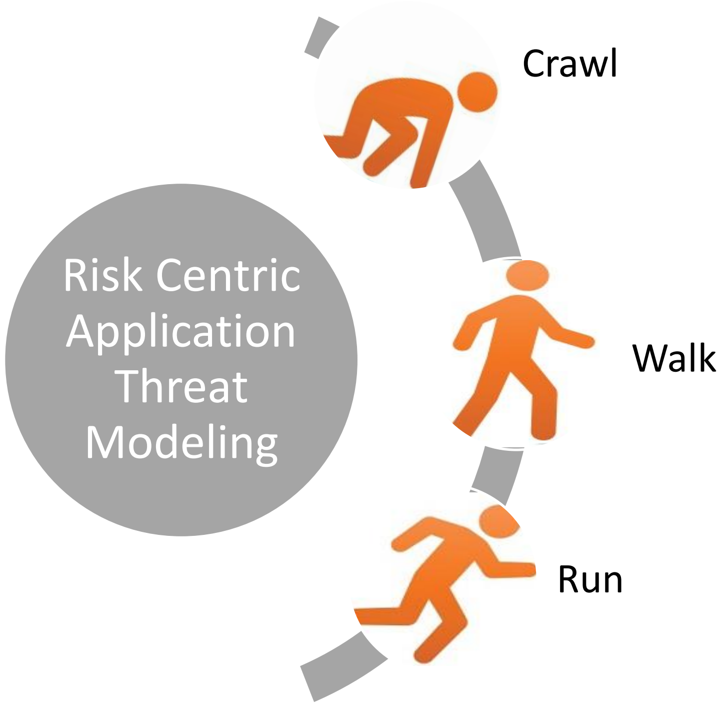


Security Testing
Security Operations Group
Scope of Web Application Environments
Results Generated
Results Reviewed For Accuracy
Produce Deliverables
Technical Vulnerability Reports
Share Results
Threat Modeler
Integrate into Attack Tree
Identify Risk Issues from Threat Model

PASTA Adoption

Phased Approaches for New Entities

- ❑ Provides for a flexible, phased approach for adoption of application threat modeling
- ❑ Simplifies threat modeling activities across 7 possible stages
- ❑ Integrates with risk management efforts within various product groups
- ❑ Informal adoption models: crawl-walk-run
- ❑ Can tie to BSIMM or OpenSAMM



Leveraging Security Incidents to Feed a PASTA Threat Model

Threat Model Case Study Consumer Electronics (IoT)

CloudPets Background

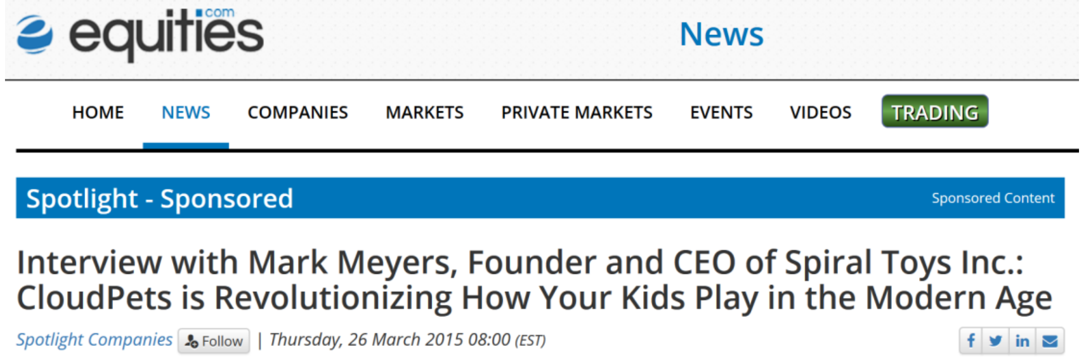
- CloudPets Data Exfiltration Case
  - Product is a stuffed animal that interfaces to a Cloud based APIs and interfaces with mobile client apps
  - Childrens recording data was efiltrated and crimnals attempted to extort victims media captured.
  - Attack vector was an exposed MongoDB interface that was available from the web w/o proper authentication.
  - {Advertised} "**CloudPets** bring you a whole NEW way to do messaging, play games, listen to lullabies and - coming soon -stories too!"

CLOUDPETS/CNNMONEY

CloudPets –Stage I IoT Example

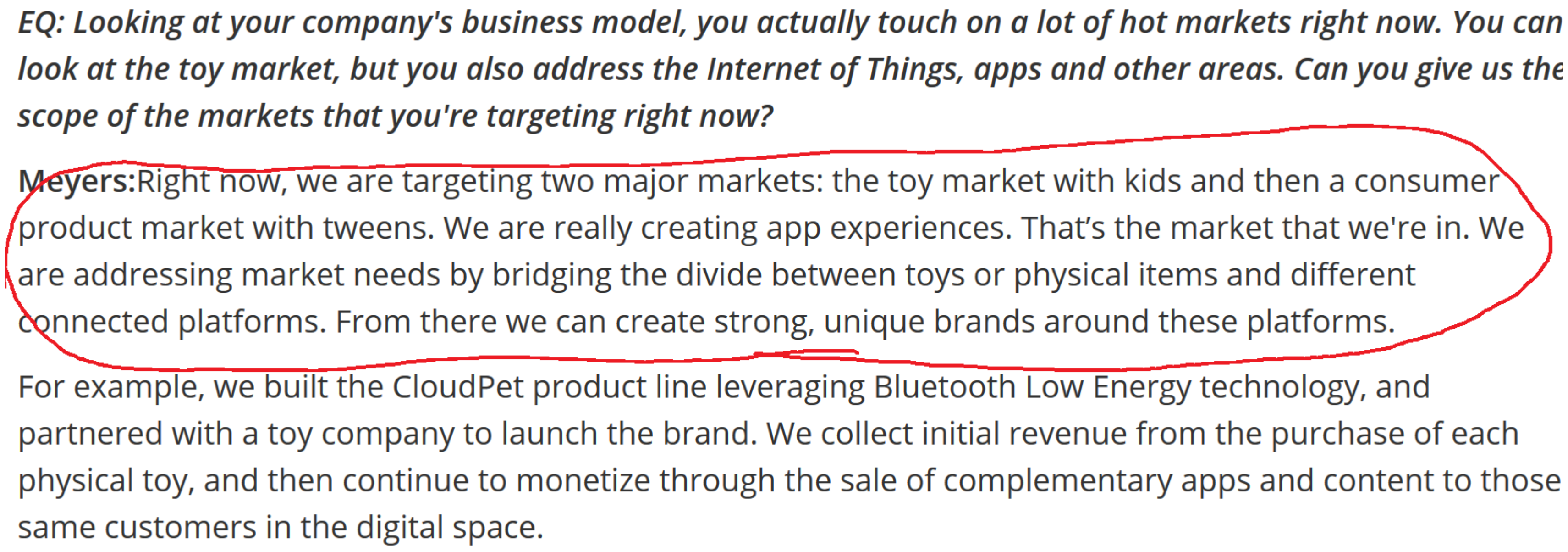
(S1) – Understanding Biz Obj of App

- “App Experiences”
  - PII Needed
  - Internet accessible APIs
  - Web enabled technologies in physical consumer electronics
  - “Parents and family members are able to participate in the child’s day-to-day playtime from



Interview with Mark Meyers, Founder and CEO of Spiral Toys Inc.: CloudPets is Revolutionizing How Your Kids Play in the Modern Age

Spotlight Companies Follow | Thursday, 26 March 2015 08:00 (EST)



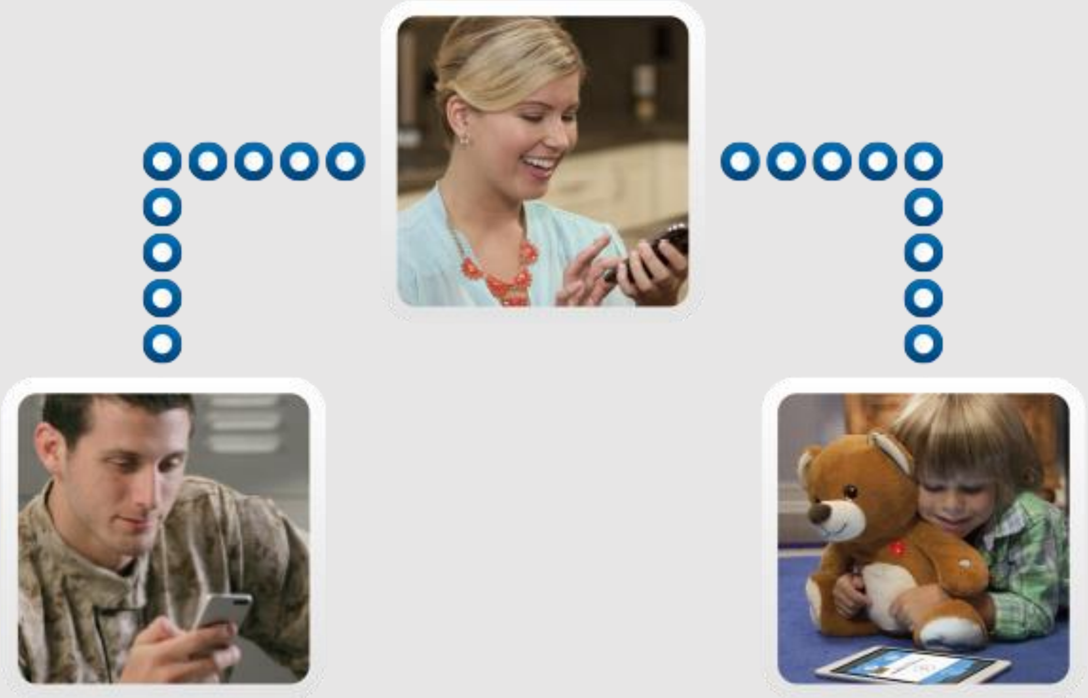
EQ: Looking at your company's business model, you actually touch on a lot of hot markets right now. You can look at the toy market, but you also address the Internet of Things, apps and other areas. Can you give us the scope of the markets that you're targeting right now?

Meyers: Right now, we are targeting two major markets: the toy market with kids and then a consumer product market with tweens. We are really creating app experiences. That’s the market that we're in. We are addressing market needs by bridging the divide between toys or physical items and different connected platforms. From there we can create strong, unique brands around these platforms.

For example, we built the CloudPet product line leveraging Bluetooth Low Energy technology, and partnered with a toy company to launch the brand. We collect initial revenue from the purchase of each physical toy, and then continue to monetize through the sale of complementary apps and content to those same customers in the digital space.

Objectives to Threats :: Stage I to IV Mapping

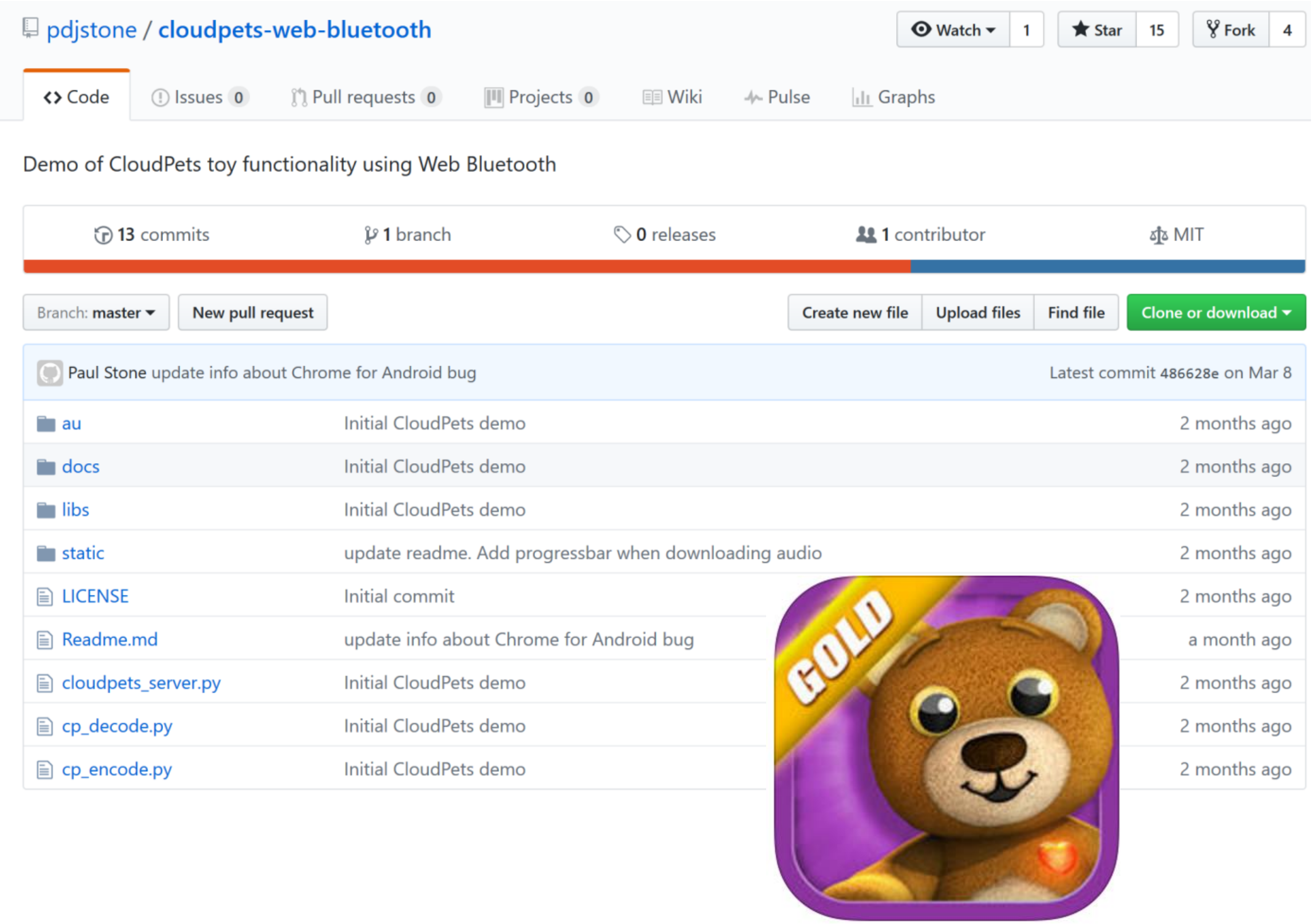
- App Components –> Use Case Mappings Unique app experiences
  - Provide inter-operability with multiple computing platforms
- Threats to Objectives
  - IP Theft
  - Application DoS
  - Application DoS
  - Expanded Attack Surface affecting security & privacy



CloudPets – an IoT PASTA Threat Model Stage II Technology Enumeration (Define Attack Surface)

(S2) – Define Technology Scope/ Attack Surface

- Device Attack Surface
  - Web Bluetooth Low Energy (BLE)
  - Mobile Application Client
- Web Service Attack Surface
  - Nginx 1.10
  - Ubuntu Server
  - Exposed web service
- Actors
  - Unauthenticated actor
- Sample Use Cases
  - "Lullabies – Upload a lullaby song to your child's CloudPets toy"
  - "Stories - Read 2, full length children's stories with your child.
    - Follow along in the app as the story is read by a narrator."
  - Connect/ Disconnect [to Toy]
  - LED On/Off (Control Toy)
  - sendAudio (to Toy) (slot1/2)
  - Send Record Command w/ Toy Microphone



pdjstone / cloudpets-web-bluetooth

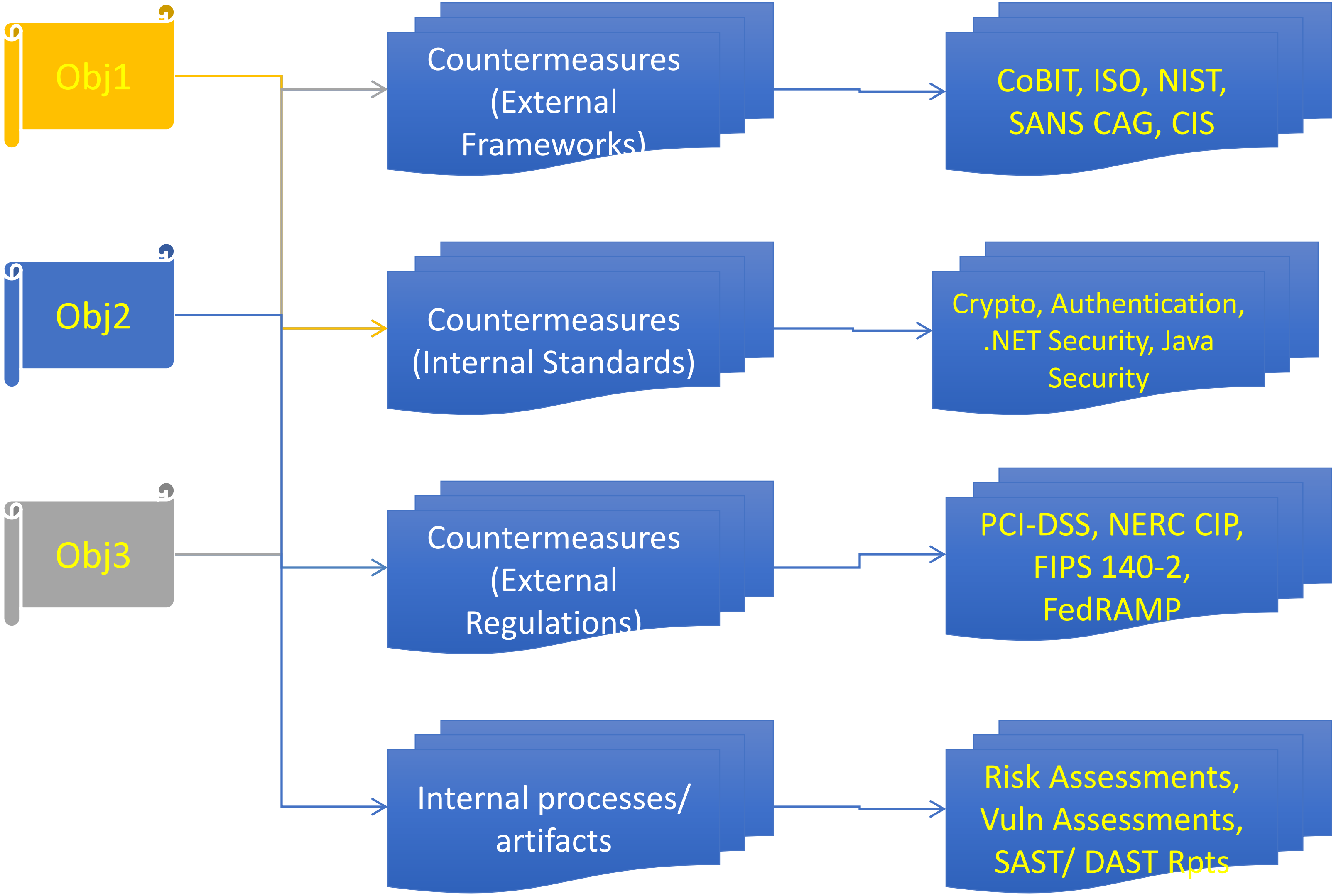
Demo of CloudPets toy functionality using Web Bluetooth

13 commits · 1 branch · 0 releases · 1 contributor · MIT

Paul Stone update info about Chrome for Android bug — Latest commit 486628e on Mar 8

au	Initial CloudPets demo	2 months ago
docs	Initial CloudPets demo	2 months ago
libs	Initial CloudPets demo	2 months ago
static	update readme. Add progressbar when downloading audio	2 months ago
LICENSE	Initial commit	2 months ago
Readme.md	update info about Chrome for Android bug	a month ago
cloudpets_server.py	Initial CloudPets demo	2 months ago
cp_decode.py	Initial CloudPets demo	2 months ago
cp_encode.py	Initial CloudPets demo	2 months ago

Pre-Emptive Security via PASTA – Stage 1



Obj1

Obj2

Obj3

Countermeasures (External Frameworks)

CoBIT, ISO, NIST, SANS CAG, CIS

Countermeasures (Internal Standards)

Crypto, Authentication, .NET Security, Java Security

Countermeasures (External Regulations)

PCI-DSS, NERC CIP, FIPS 140-2, FedRAMP

Internal processes/ artifacts

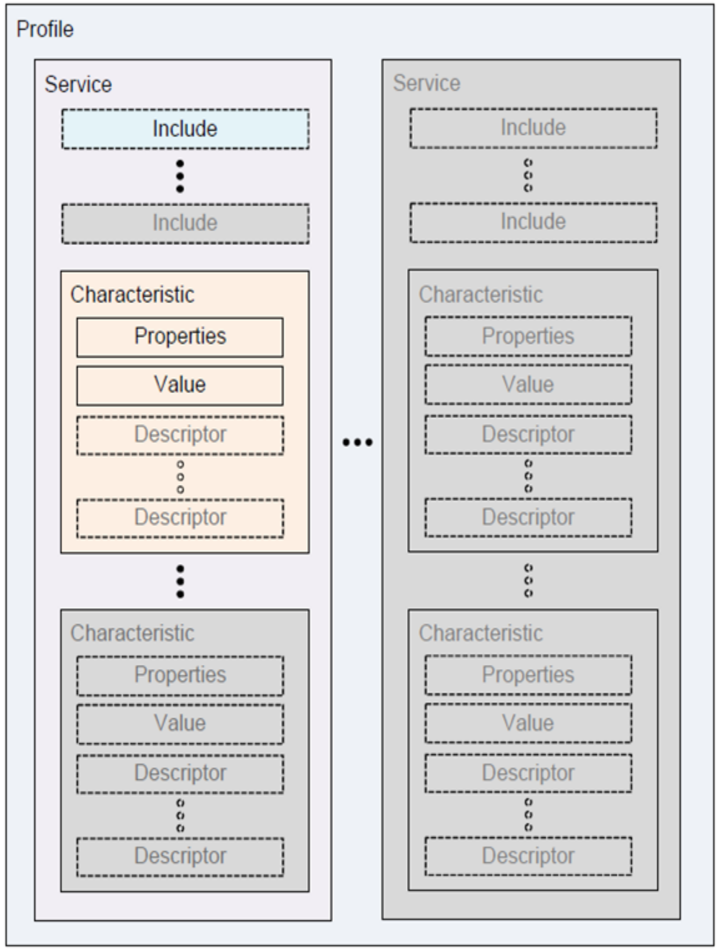
Risk Assessments, Vuln Assessments, SAST/ DAST Rpts

Scoping an Attack Surface in PASTA’s Stage II

- Defines technology footprint for those involved in threat model
  - AD servers, Databases (relational/ flat file), Infrastructure, Web services (MS-WSE, WCF, REST API, JavaScript, Frameworks (OpenMEAP, etc.))
  - ARM related technology – vendor or internal?
  - Includes scope of communication protocols to be used (SSL, SSH, Bluetooth, etc.)
  - Provides scope for testing and threat analysis
- Allows opportunity for security hardening to take place
  - OEM security standards applied
  - Control frameworks leveraged (OWASP Mobile Top Ten)
  - Security primer as foundation is applied
- Tools used
  - Netstat –an (Mobile), Nmap, Dpkg, ProcessExplorer, mobile auditing software, MDM solutions
  - Application architecture schematics

Application Decomposition of CloudPets Device

- Generic Attributes (GATT) define a hierarchical data structure that is exposed to connected Bluetooth LE devices.
- Device access is powerfull
- Trusted servers can serve malicious code (i.e. – XSS)
- navigator.bluetooth.getAvailability() exposes whether a Bluetooth radio is available on the user's system.



Profile

Service

Include

Include

Characteristic

Properties

Value

Descriptor

Descriptor

Characteristic

Properties

Value

Descriptor

Descriptor

Service

Include

Include

Characteristic

Properties

Value

Descriptor

Descriptor

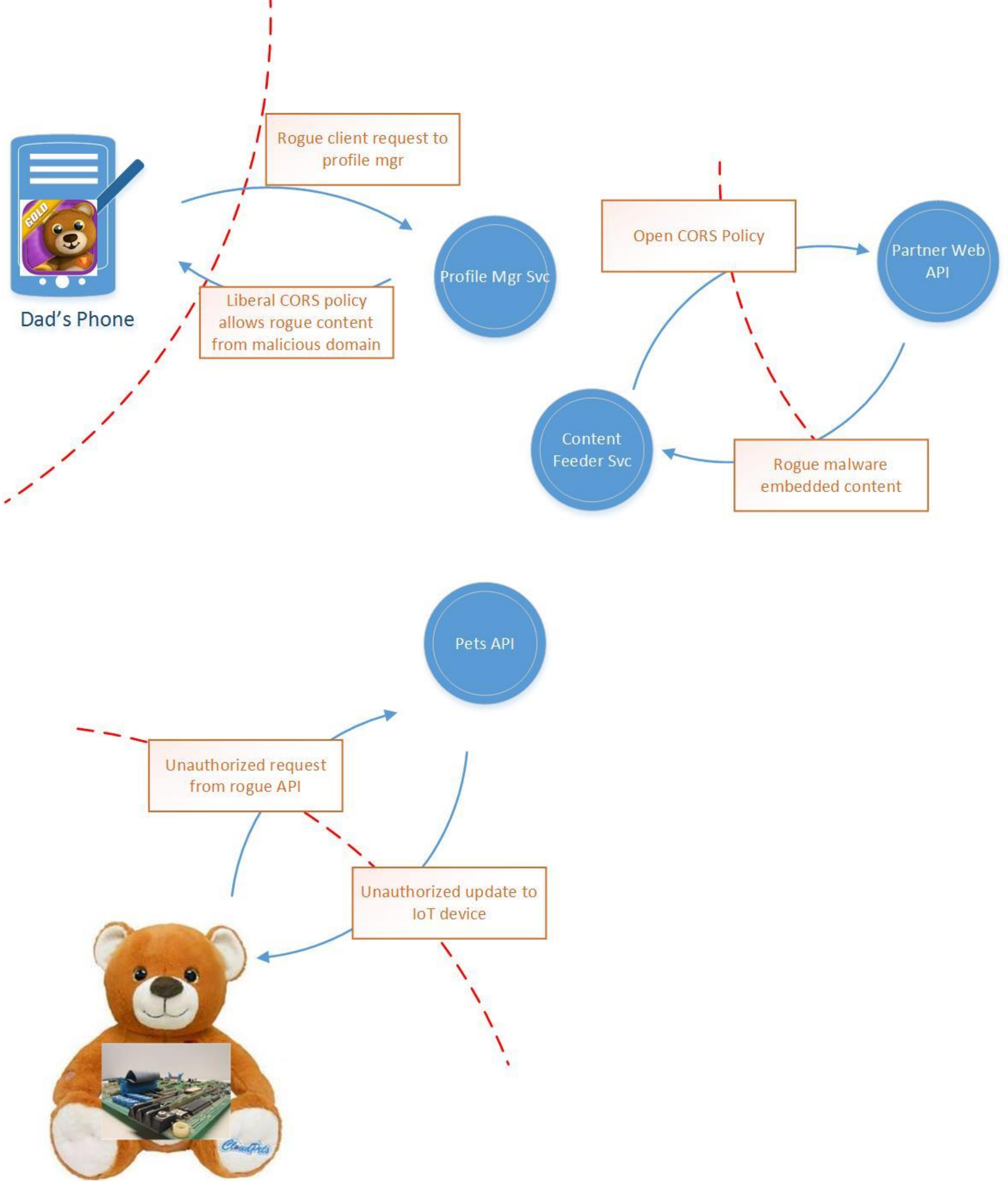
Characteristic

Properties

Value

Descriptor

Descriptor



Dad's Phone

Rogue client request to profile mgr

Liberal CORS policy allows rogue content from malicious domain

Profile Mgr Svc

Open CORS Policy

Partner Web API

Content Feeder Svc

Rogue malware embedded content

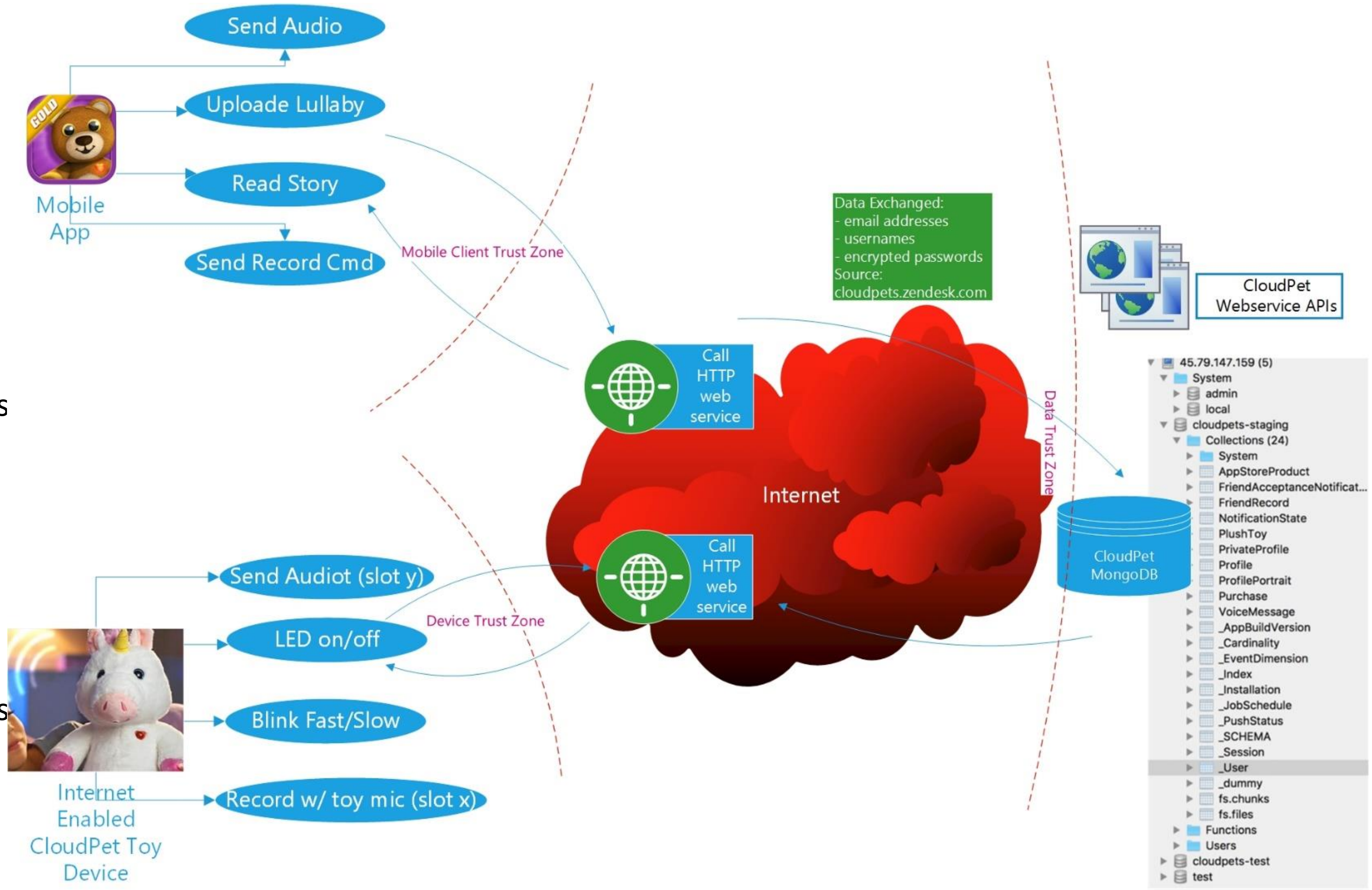
Pets API

Unauthorized request from rogue API

Unauthorized update to IoT device

CloudPets –IoT PASTA Threat Model Stage III (Application Decomposition)

- Stage III of PASTA incorporates DFDs
- Begin with use cases
  - Map actors
  - Map technology components
  - Understand data flows
  - Begin to map out trust boundaries
  - Tech components may have underlying use cases not used by the product



Data Exchanged:
- email addresses
- usernames
- encrypted passwords
Source:
cloudpets.zendesk.com

```
▼ 45.79.147.159 (5)
  ▼ System
    ▶ admin
    ▶ local
  ▼ cloudpets-staging
    ▼ Collections (24)
      ▶ System
      ▶ AppStoreProduct
      ▶ FriendAcceptanceNotificat...
      ▶ FriendRecord
        NotificationState
        PlushToy
        PrivateProfile
        Profile
        ProfilePortrait
      ▶ Purchase
      ▶ VoiceMessage
      ▶ _AppBuildVersion
      ▶ _Cardinality
      ▶ _EventDimension
      ▶ _Index
      ▶ _Installation
      ▶ _JobSchedule
      ▶ _PushStatus
      ▶ _SCHEMA
      ▶ _Session
      ▶ _User
      ▶ _dummy
      ▶ fs.chunks
      ▶ fs.files
    ▶ Functions
    ▶ Users
  ▶ cloudpets-test
  ▶ test
```

Beyond Application Decomposition in Stage III

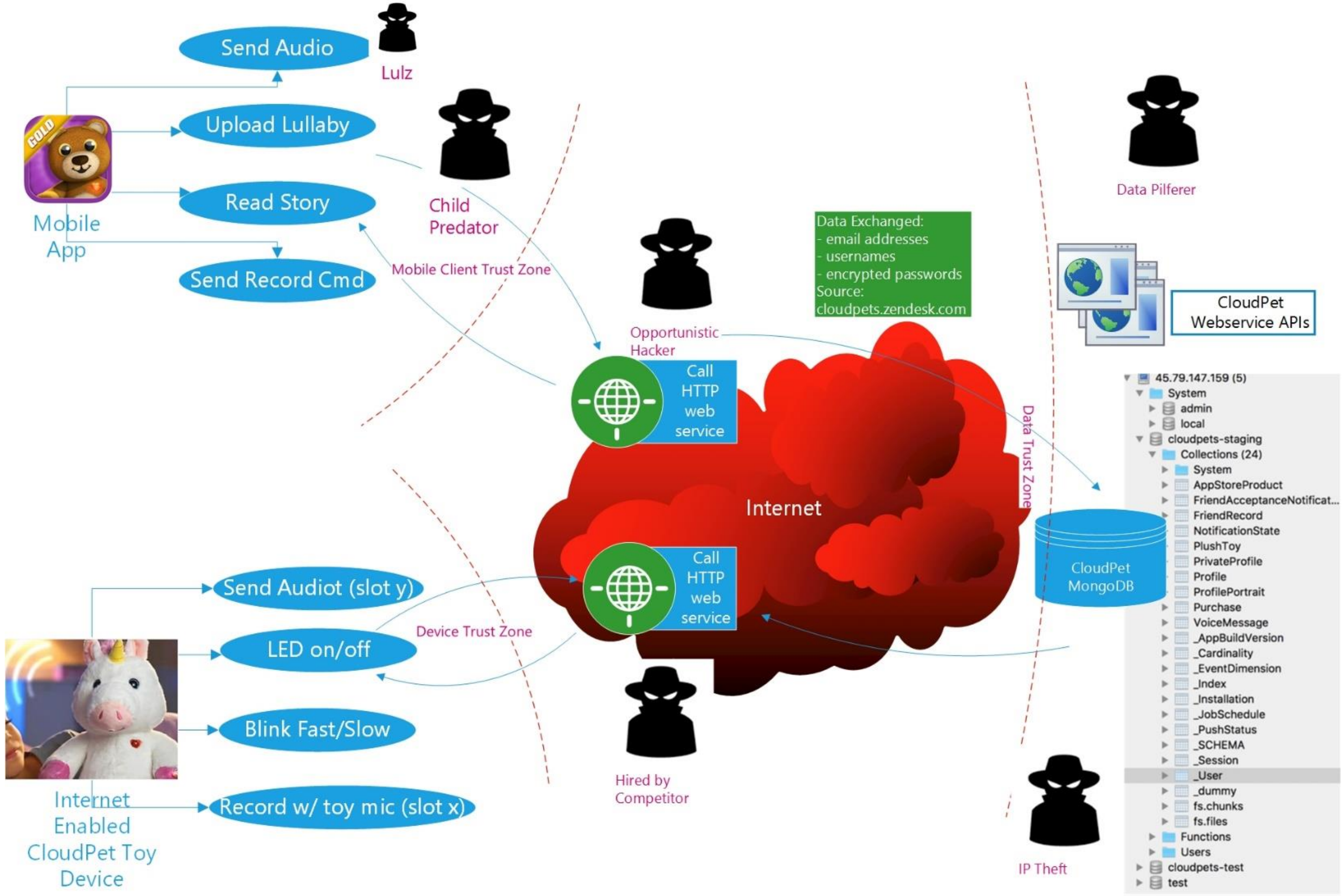
Decomposing Application Stack

- ❑ Assets can encompass several components
  - Drivers, HW Interfaces, O/S, running services, etc.
- ❑ Host based component enumeration also useful (installed S/W, packages, embedded systems)
- ❑ Smallest component can be backdoor
  - Hacker: Fake signed driver update
  - End User: ‘It’s a driver update only’

```
•  E:\ubuntu_64_hw_sw\ubuntu_64_hw_sw\pci_hardware

•  00:00.0 Host bridge: Intel Corporation 440BX/ZX/DX -
   82443BX/ZX/DX Host bridge (rev 01)

•  00:01.0 PCI bridge: Intel Corporation 440BX/ZX/DX -
   82443BX/ZX/DX AGP bridge (rev 01)

•  00:07.0 ISA bridge: Intel Corporation 82371AB/EB/MB PIIX4
   ISA (rev 08)

•  00:07.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4
   IDE (rev 01)

•  00:07.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI
   (rev 08)

•  00:07.7 System peripheral: VMware Virtual Machine
   Communication Interface (rev 10)

•  00:0f.0 VGA compatible controller: VMware SVGA II Adapter

•  00:10.0 SCSI storage controller: LSI Logic / Symbios Logic
   53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI (rev 01)

•  00:11.0 PCI bridge: VMware PCI bridge (rev 02)

•  ...

•  00:18.2 PCI bridge: VMware PCI Express Root Port (rev 01)

•  00:18.3 PCI bridge: VMware PCI Express Root Port (rev 01)

•  00:18.4 PCI bridge: VMware PCI Express Root Port (rev 01)

•  00:18.5 PCI bridge: VMware PCI Express Root Port (rev 01)

   00:18.6 PCI bridge: VMware PCI Express Root Port (rev 01)
```

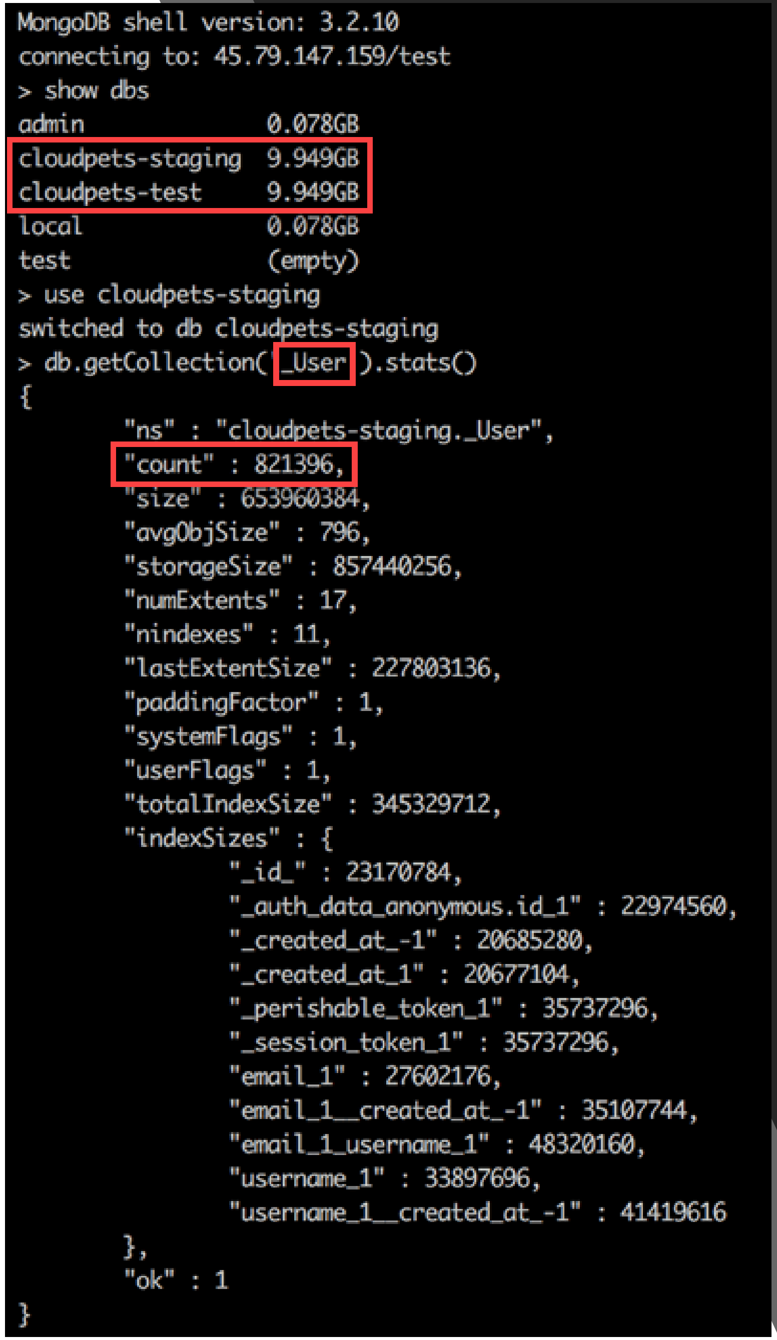
CloudPets –IoT PASTA Threat Model Stage IV (Threat Analysis)

- Leverage threat intel for consumer electronics
- Leverage threat intel for IT Infrastructure (IT-ISAC)
- Identify abuse cases
  - Lulz
  - Child Predator
  - IP Theft
  - Corporate Sabotage
  - Data extraction
  - Ransom/ Extortion



Data Exchanged:
- email addresses
- usernames
- encrypted passwords
Source:
cloudpets.zendesk.com

```
▼ 45.79.147.159 (5)
  ▼ System
    ▶ admin
    ▶ local
  ▼ cloudpets-staging
    ▼ Collections (24)
      ▶ System
      ▶ AppStoreProduct
      ▶ FriendAcceptanceNotificat...
      ▶ FriendRecord
      ▶ NotificationState
      ▶ PlushToy
      ▶ PrivateProfile
      ▶ Profile
      ▶ ProfilePortrait
      ▶ Purchase
      ▶ VoiceMessage
      ▶ _AppBuildVersion
      ▶ _Cardinality
      ▶ _EventDimension
      ▶ _Index
      ▶ _Installation
      ▶ _JobSchedule
      ▶ _PushStatus
      ▶ _SCHEMA
      ▶ _Session
      ▶ _User
      ▶ _dummy
      ▶ fs.chunks
      ▶ fs.files
    ▶ Functions
    ▶ Users
  ▶ cloudpets-test
  ▶ test
```



```
MongoDB shell version: 3.2.10
connecting to: 45.79.147.159/test
> show dbs
admin              0.078GB
cloudpets-staging  9.949GB
cloudpets-test     9.949GB
local              0.078GB
test               (empty)
> use cloudpets-staging
switched to db cloudpets-staging
> db.getCollection('_User').stats()
{
        "ns" : "cloudpets-staging._User",
        "count" : 821396,
        "size" : 653960384,
        "avgObjSize" : 796,
        "storageSize" : 857440256,
        "numExtents" : 17,
        "nindexes" : 11,
        "lastExtentSize" : 227803136,
        "paddingFactor" : 1,
        "systemFlags" : 1,
        "userFlags" : 1,
        "totalIndexSize" : 345329712,
        "indexSizes" : {
                "_id_" : 23170784,
                "_auth_data_anonymous.id_1" : 22974560,
                "_created_at_-1" : 20685280,
                "_created_at_1" : 20677104,
                "_perishable_token_1" : 35737296,
                "_session_token_1" : 35737296,
                "email_1" : 27602176,
                "email_1__created_at_-1" : 35107744,
                "email_1_username_1" : 48320160,
                "username_1" : 33897696,
                "username_1__created_at_-1" : 41419616
        },
        "ok" : 1
}
```

PASTA Stage IV Threat Scenarios to Data Use Case Mapping

- Correlate threat scenarios from threat library (in DB) to answers provided by user around app via a questionnaire
- Provide likely threat scnearios from a static threat library based upon the following:
  - Industry to which the application pertains to
  - Architectural level of subject application
  - Data types managed by application
  - Identified application components
  - Identify the threats that would serve as the hierarchical root node for an attack tree
    - Provision a container for the tool
    - Execute the tool using the supplied command
    - Process/transform the result using the defined transformation utility
    - Provide the standardized result
- Import threat intelligence feeds from various sources (e.g. - US Cert, FS-ISAC, IT-ISAC, RISC, etc) in order to consider the latest threat scenarios

PASTA's Stage IV – Threat Analysis & Categorization

Spoofing/ Impersonation
- Impersonate vendor
- Impersonate app actor
- Impersonate domain/ network actor
- Impersonate employee
- Impersonate trusted relationship

Tampering of Data
- Affect financial information
- Alter criminal records
- Alter scholastic records
- Alter legal records
- Alter product/ device functionality
- Alter integrity of software
- Alter medical records

Repudiation
- Erase online criminal activity
- Anonymized online activity
- Erase log information

Denial of Service
- DoS
- DDoS
- Application Logic Bombs
- Bots looping POST requests

Elevation of Privileges
- Elevate to actor privileges on app level
- Elevate to actor privileges on system level
- Change data in database

Extortion
- Get Money
- Political blackmail.

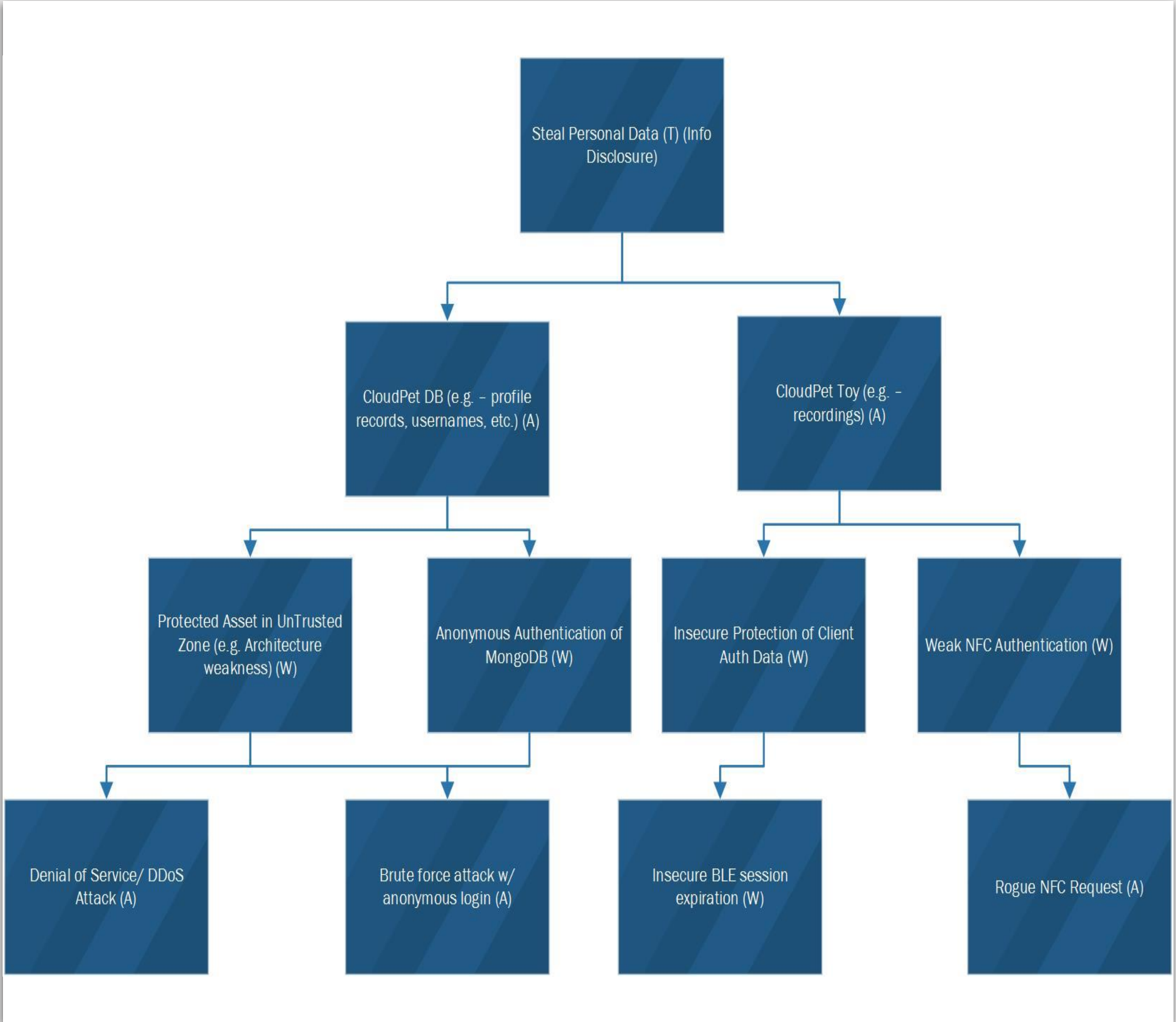
Research
- Exploit dev for hire
- Lulz
- Online credentials
- Corporate espionage
- Create exploit kit/ botnet

CloudPets Threat Model :: Stages V & VI

- Vulnerability Analysis
  - Security Architecture
  - CRUD Exercises
  - Application Security (Authentication focus)
  - System/ DB Security
- Exploit Testing
  - Build attack tree
  - Conduct series of attacks based upon identified weaknesses/ vulns
  - ‘Tag’ exploitable vulns
    - Probabilistic analysis
  - Attacks based upon threats in attack tree
- Remediation prioritization based upon exploitability

CloudPets Case Mapping Possible Weaknesses in an IoT Attack Tree. (Stage V)

- Application may have multiple threats
- Multiple trees per app based upon # of threats
- Attack tree helps to blueprint attack path against defined attack surface
- Exploitation phase ‘legitimizes’ attack – tests for viability
- Leverage CAPEC to CWE mapping for ease of use



Steal Personal Data (T) (Info Disclosure)

CloudPet DB (e.g. – profile records, usernames, etc.) (A)

CloudPet Toy (e.g. – recordings) (A)

Protected Asset in UnTrusted Zone (e.g. Architecture weakness) (W)

Anonymous Authentication of MongoDB (W)

Insecure Protection of Client Auth Data (W)

Weak NFC Authentication (W)

Denial of Service/ DDoS Attack (A)

Brute force attack w/ anonymous login (A)

Insecure BLE session expiration (W)

Rogue NFC Request (A)

Stage VII – Residual Risk Analysis

- Identify most realistic threats
    - Map identified weaknesses or vulnerabilities
    - Map relevant attack patterns
        - Test attack patterns
    - Conduct probabilistic analysis on Threats and Vulnerabilities
    - Determine aggregate impact
- Prioritization on remediation focused on risk level, not CWE or CVE
- Risk analysis reflects collaborative approach via PASTA

Mobile Application Case Study
PASTA model for mobile applications

PASTA Stage I – BIA on Mobile Applications

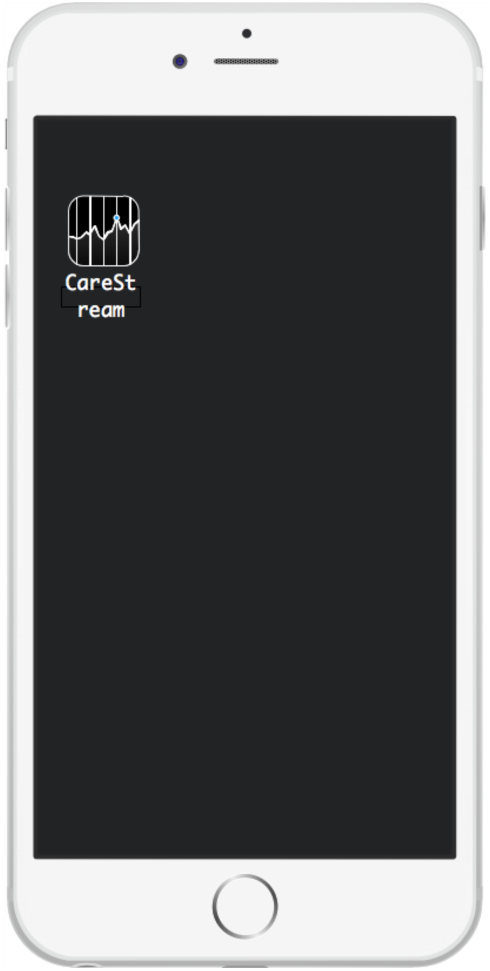
Business Objectives

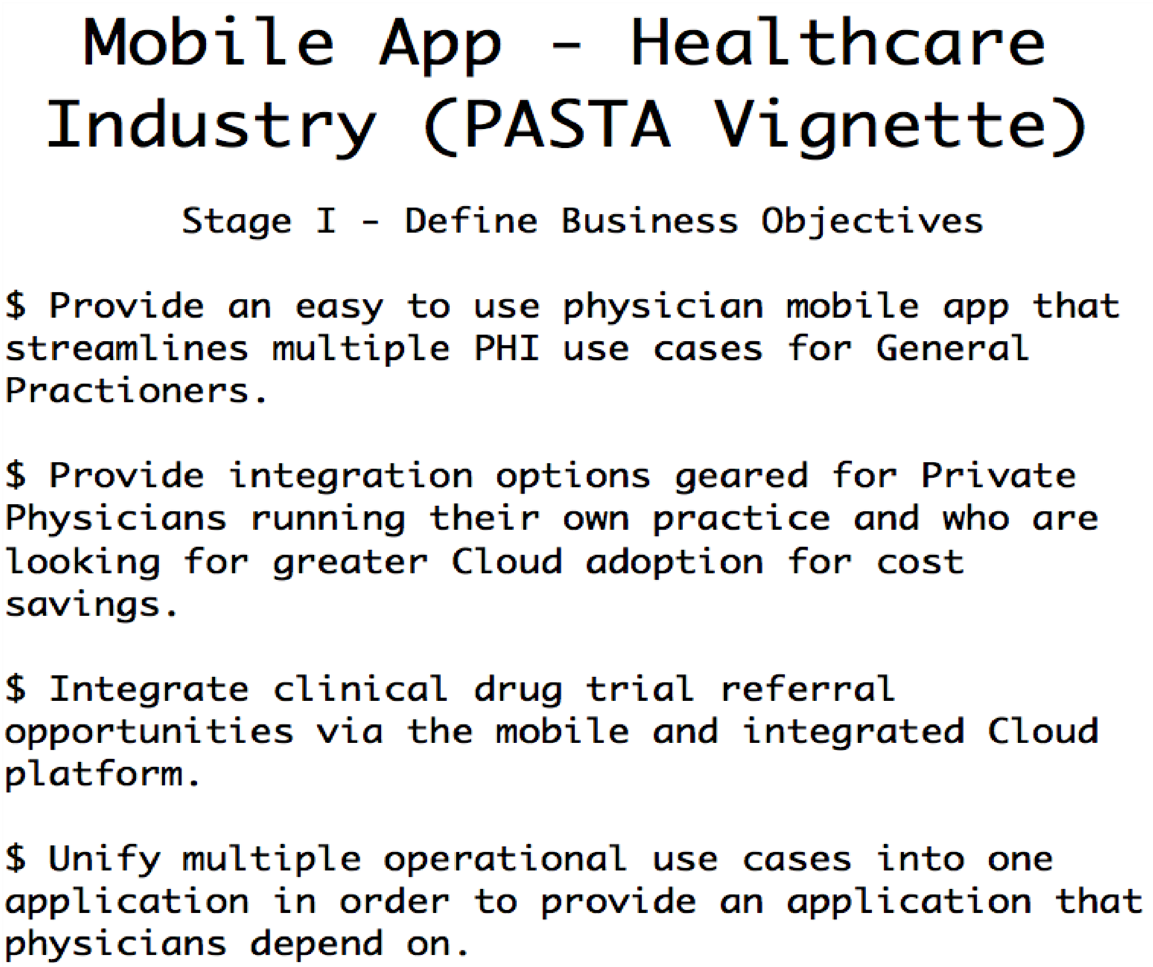
- Increased sales
- Brand awareness
- Cross sale opportunities
- Establish solid reputation as mobile software development company
- Gain loyalty in mobile app followers
- Key metrics
  - # downloads
  - # accounts
  - # of active accounts

Security Considerations

- Address regulatory requirements early
- SW Objectives
  - Reliable Design Frameworks
  - Good Design Patterns
  - Availability
  - Data Integrity
  - Confidentiality
- Secure App Components
  - Key APIs, data sources

Deriving Impact from Mobile App Use Cases





Mobile App - Healthcare Industry (PASTA Vignette)

Stage I - Define Business Objectives

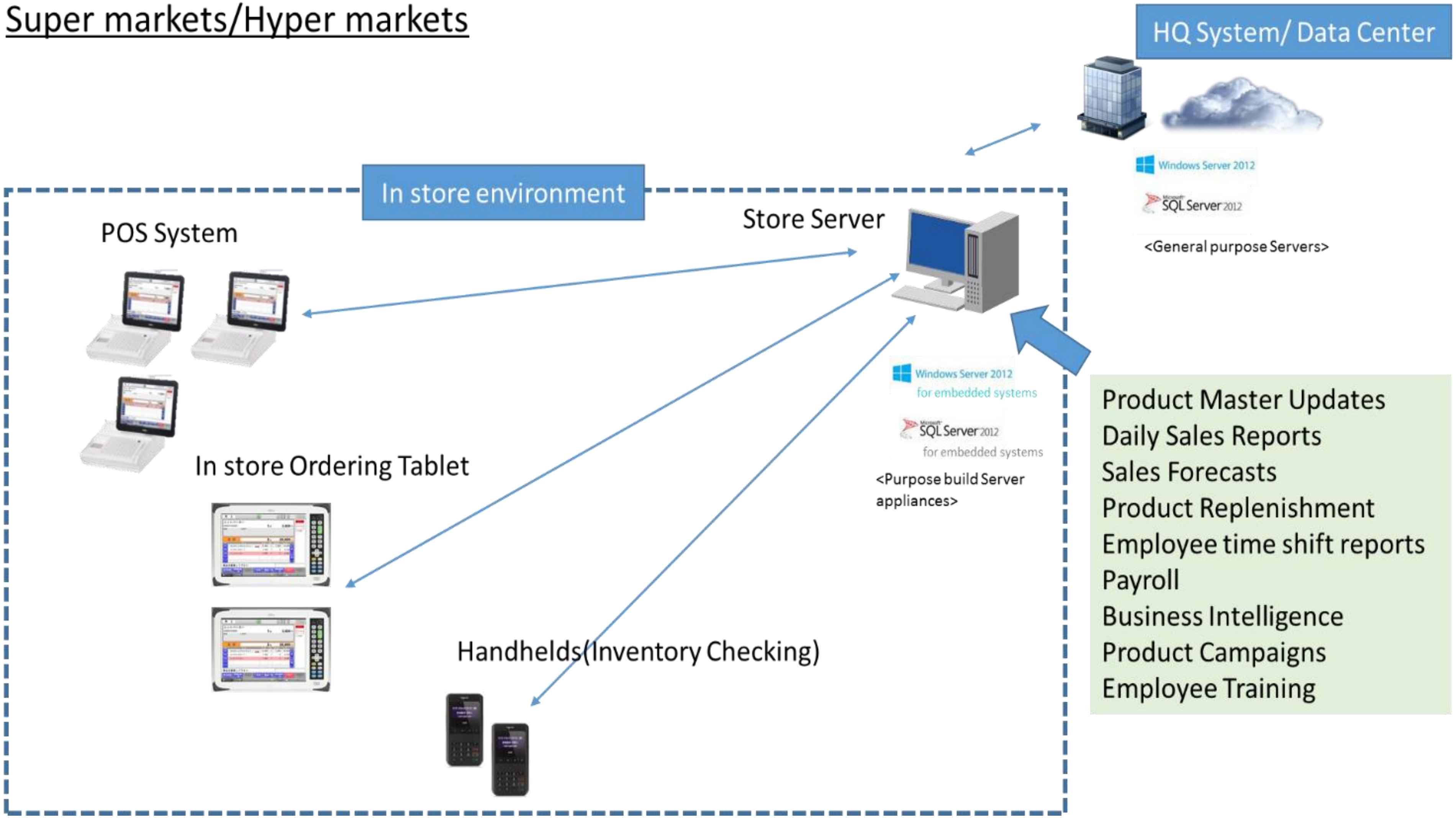
$ Provide an easy to use physician mobile app that streamlines multiple PHI use cases for General Practioners.

$ Provide integration options geared for Private Physicians running their own practice and who are looking for greater Cloud adoption for cost savings.

$ Integrate clinical drug trial referral opportunities via the mobile and integrated Cloud platform.

$ Unify multiple operational use cases into one application in order to provide an application that physicians depend on.

You Can’t Protect What You Don’t Know



System and Store Server Functionality overview in Convenience Stores, Super markets/Hyper markets

HQ System/ Data Center

Windows Server 2012

SQL Server 2012

<General purpose Servers>

In store environment

POS System

Store Server

Windows Server 2012 for embedded systems

SQL Server 2012 for embedded systems

<Purpose build Server appliances>

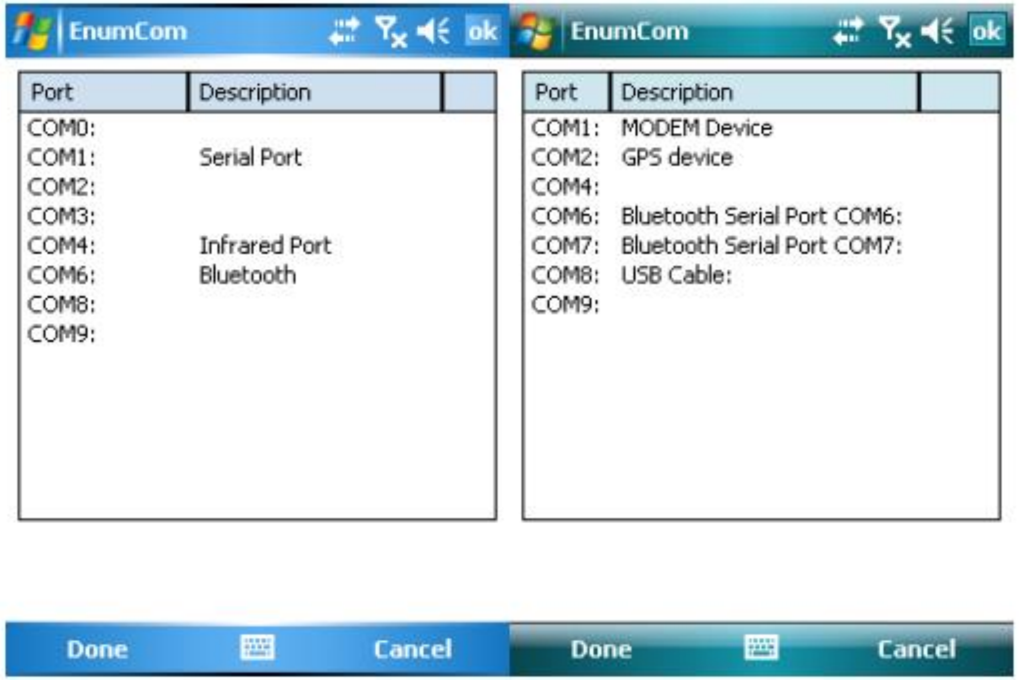
In store Ordering Tablet

Handhelds(Inventory Checking)

Product Master Updates
Daily Sales Reports
Sales Forecasts
Product Replenishment
Employee time shift reports
Payroll
Business Intelligence
Product Campaigns
Employee Training

Know Your Mobile ‘Assets’

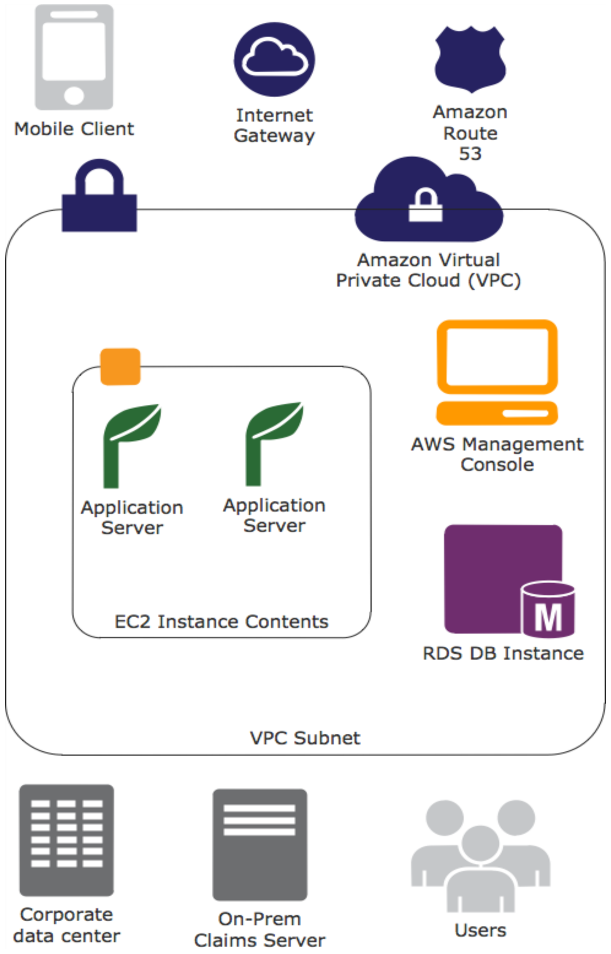
- Focuses on listing technology used in mobile app; enumeration exercise
- Platform: Android, Blackberry, iOS, Windows Phone, Asha, Sailfish OS, etc.
- Mobile Application Features
  - NFC
  - Bluetooth
  - GPS
  - Camera
  - Microphone
  - Sensors
  - USB
- Architectural components
  - Server platforms, OS, App Server, DB, etc.
  - Infrastructure (DNS, Proxies, Firewalls, etc.)

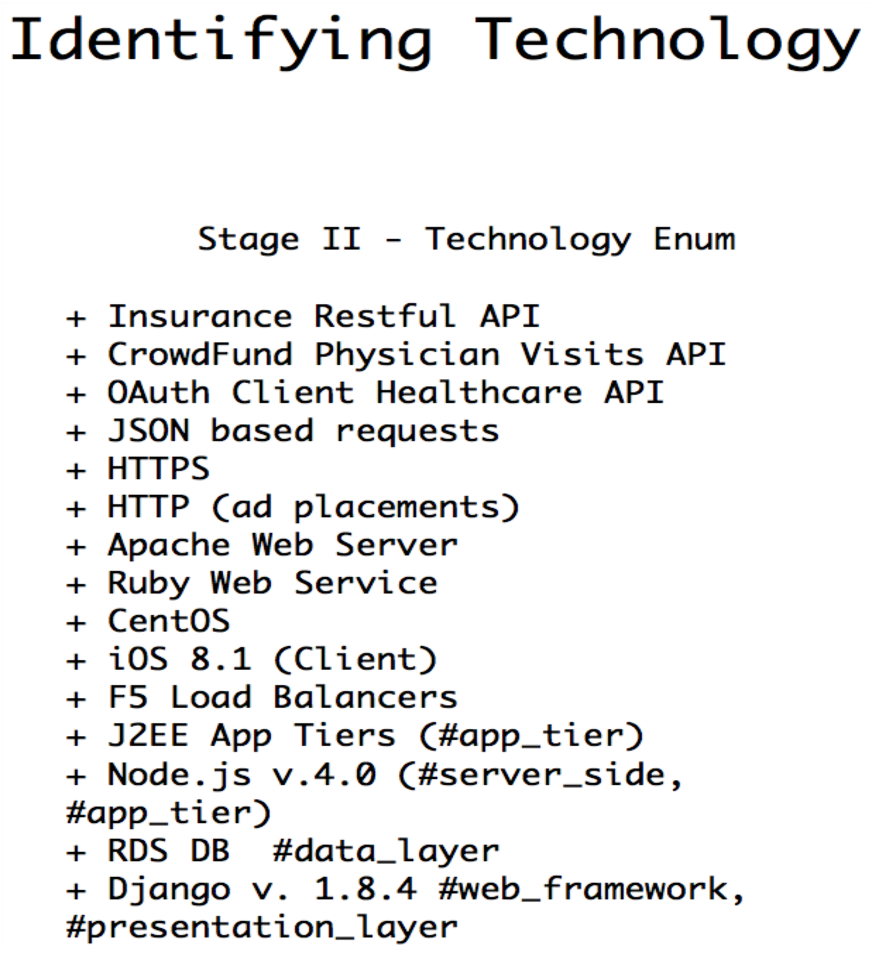


Port	Description
COM0:	
COM1:	Serial Port
COM2:	
COM3:	
COM4:	Infrared Port
COM6:	Bluetooth
COM8:	
COM9:	

Port	Description
COM1:	MODEM Device
COM2:	GPS device
COM4:	
COM6:	Bluetooth Serial Port COM6:
COM7:	Bluetooth Serial Port COM7:
COM8:	USB Cable:
COM9:	

Define Scope of Protection/ Attack





Identifying Technology

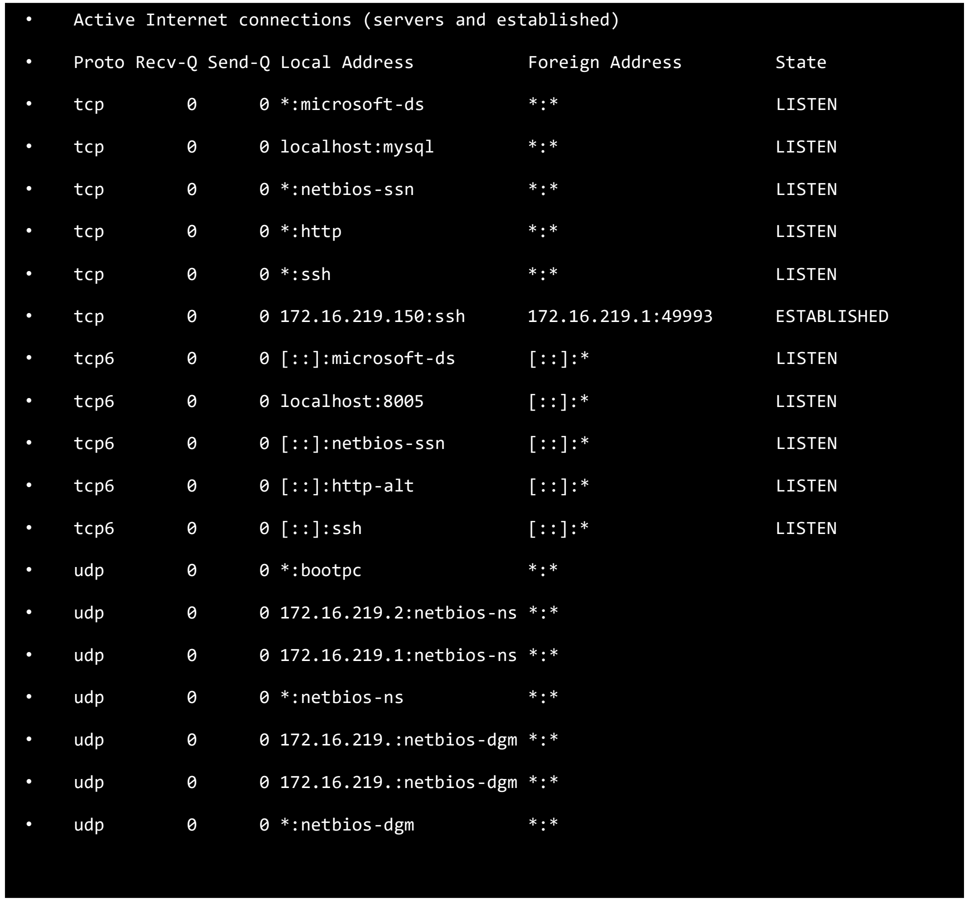
Stage II - Technology Enum

+ Insurance Restful API
+ CrowdFund Physician Visits API
+ OAuth Client Healthcare API
+ JSON based requests
+ HTTPS
+ HTTP (ad placements)
+ Apache Web Server
+ Ruby Web Service
+ CentOS
+ iOS 8.1 (Client)
+ F5 Load Balancers
+ J2EE App Tiers (#app_tier)
+ Node.js v.4.0 (#server_side, #app_tier)
+ RDS DB #data_layer
+ Django v. 1.8.4 #web_framework, #presentation_layer

PASTA Stage II – Attack Surface Creation/ Tech Enum

Identifying service components that may provide attack vector

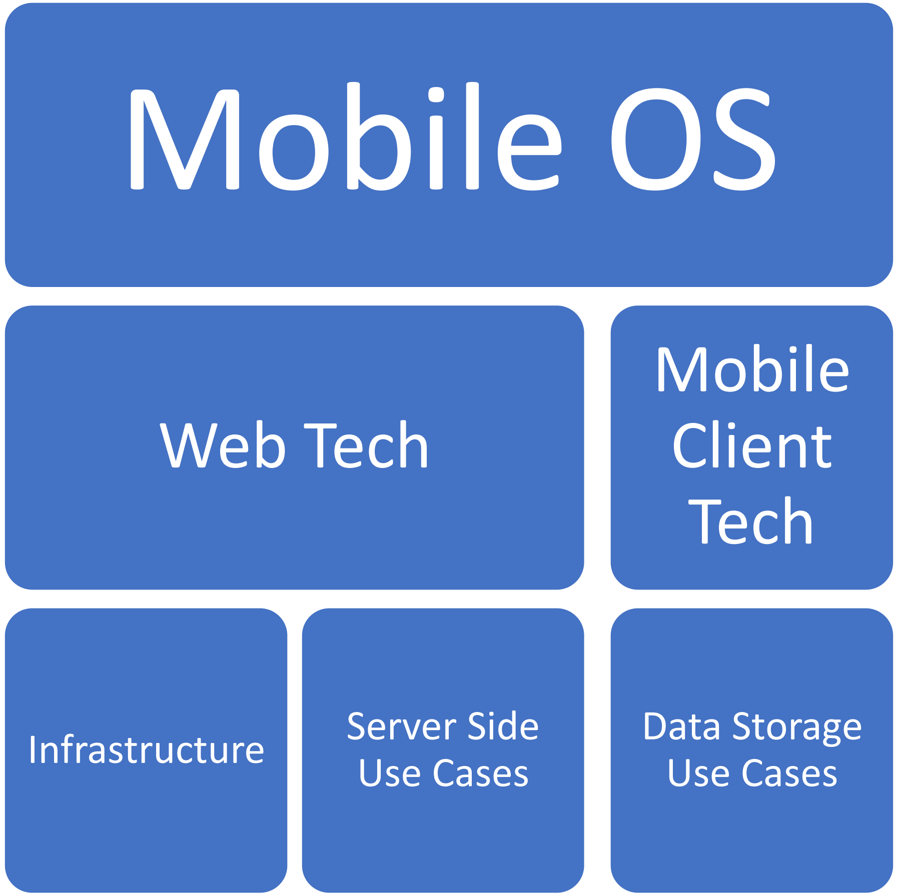
- ❑ Assets reveal what they are, what versions they have, what components they support
  - ▪ Components: system files, installed s/w, services, named pipes, compiled libraries (binaries)
- ❑ Response info fuels attacks if response reveals vulnerable components
- ❑ Security begins here: Security Hardening & Network Defenses
  - ▪ Hardened accounts
  - ▪ Detect/ prevent network scans
  - ▪ Divest unnecessary software’



```
•   Active Internet connections (servers and established)
•   Proto Recv-Q Send-Q Local Address           Foreign Address         State
•   tcp        0      0 *:microsoft-ds          *:*                     LISTEN
•   tcp        0      0 localhost:mysql         *:*                     LISTEN
•   tcp        0      0 *:netbios-ssn           *:*                     LISTEN
•   tcp        0      0 *:http                  *:*                     LISTEN
•   tcp        0      0 *:ssh                   *:*                     LISTEN
•   tcp        0      0 172.16.219.150:ssh      172.16.219.1:49993      ESTABLISHED
•   tcp6       0      0 [::]:microsoft-ds       [::]:*                  LISTEN
•   tcp6       0      0 localhost:8005          [::]:*                  LISTEN
•   tcp6       0      0 [::]:netbios-ssn        [::]:*                  LISTEN
•   tcp6       0      0 [::]:http-alt           [::]:*                  LISTEN
•   tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
•   udp        0      0 *:bootpc                *:*
•   udp        0      0 172.16.219.2:netbios-ns *:*
•   udp        0      0 172.16.219.1:netbios-ns *:*
•   udp        0      0 *:netbios-ns            *:*
•   udp        0      0 172.16.219.:netbios-dgm *:*
•   udp        0      0 172.16.219.:netbios-dgm *:*
•   udp        0      0 *:netbios-dgm           *:*
```

Mobile Application Decomposition

- ‘Dissection’ takes place all across technology stacks
- Builds upon technology scoping phases by overlaying use cases & actors
- Begin by enumerating use cases/ actors per technology areas of architecture
  - Use cases = Activities in mobile
  - Identify manageable sub-processes & data flows
  - Android OS: Apps have unique actors per applications
  - Web APIs: App level of Integrated domain authentication
  - Use: Authentication use cases across architecture
  - Use: Encryption use cases across architecture
  - Offline vs. Online Use cases
  - Does the application perform commerce transactions?

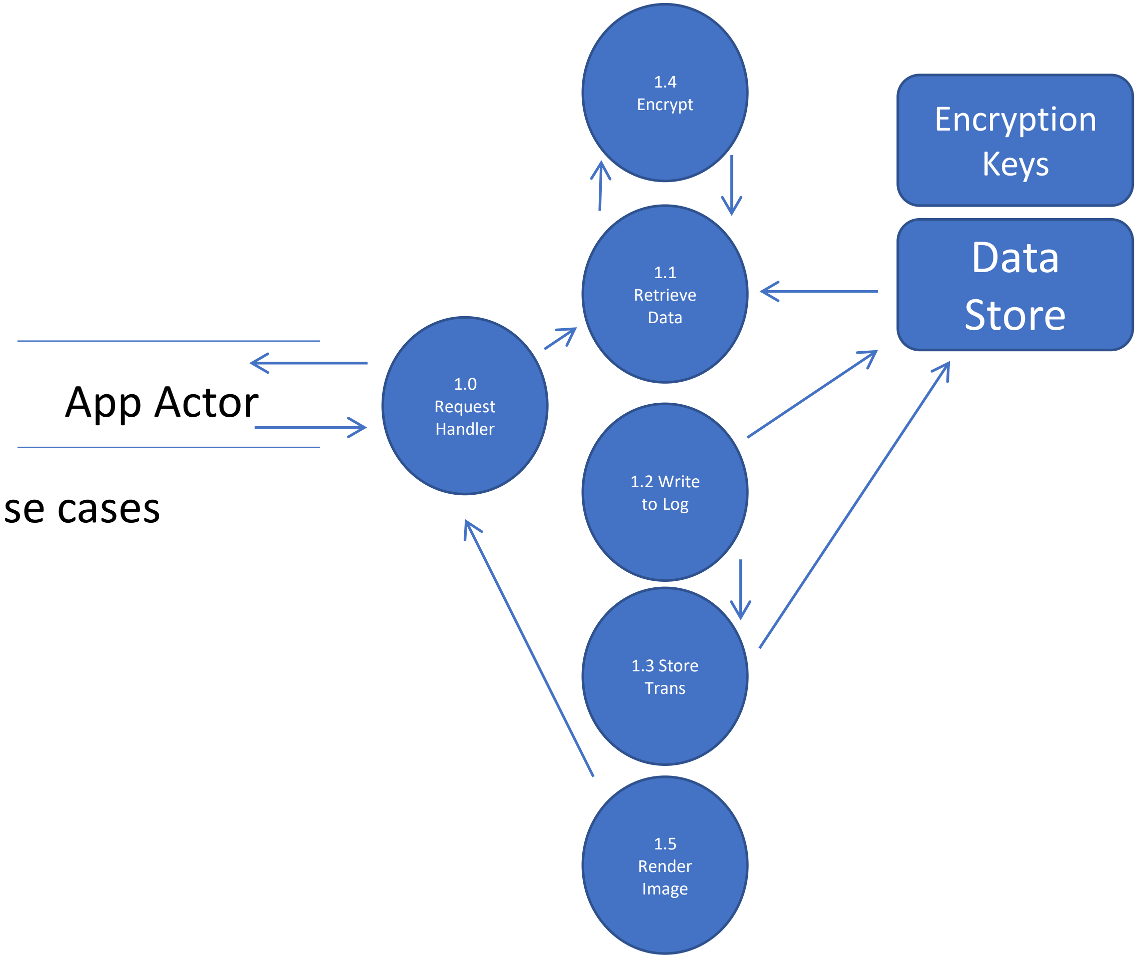


Stage III – Mapping Use Cases to Application Components

- SMS use cases need to be identified
- Voice related use cases (medical transcriptions – Dragon Dictation OK?)
- Endpoints Web Services RESTful or SOAP based
  - Third Party (Example: Amazon)
  - Websites Does the app utilize or integrate the “mobile web” version of an existing web site?
  - App Stores Google Play
  - Apple App Store
  - Windows Mobile
  - BlackBerry App Store
- Cloud Storage Amazon/Azure
- Corporate Networks (via VPN, ssh, etc.)

Mapping Call Flow (Stage III)

- ❑ Mobile Stack
  - ❑ List Activities
    - ❑ Account history request
    - ❑ DL/ render image
    - ❑ Order {x,y,z}
    - ❑ Log transaction
    - ❑ Cache image/ information
  - ❑ Map mobile elements to use cases
    - ❑ Sources
    - ❑ Sinks
    - ❑ Data stores
    - ❑ Map data flows

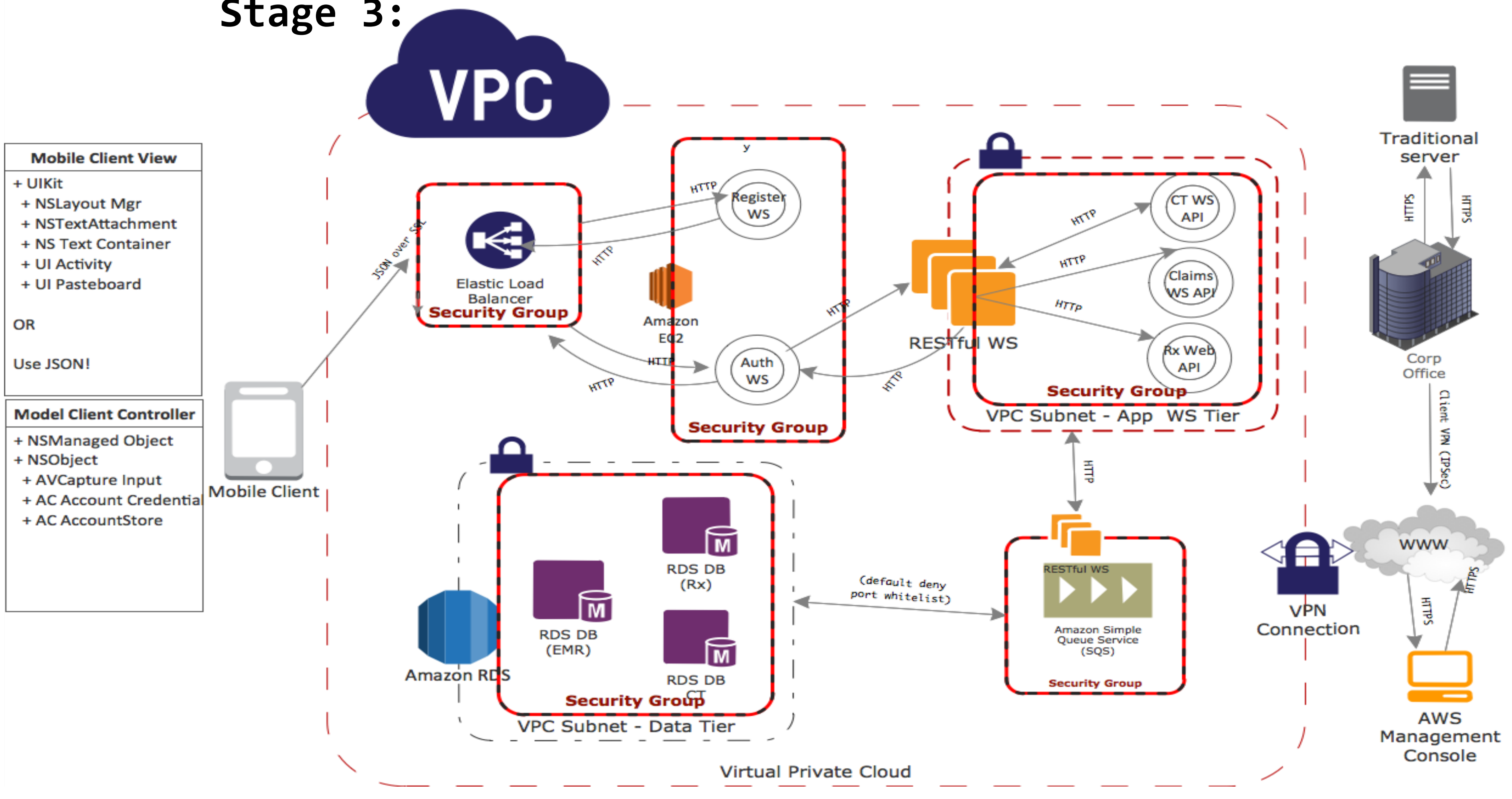


Building an Effective DFD

- **Application Components** - Services, Named Pipes, Software Libraries, etc.
- **Actors** - Human and non-Human roles interacting with a given application environment
- **Assets** - both Hardware and Software assets that interact with the application ecosystem
- **Data Repositories** - Relational databases, file systems, flat file data repositories, cached memory where data may be stored.
- **Trust Boundaries** – Although not tangible objects, they become more clearly defined as part of the process of dividing up application components

Mobile to Cloud DFD Analysis (Stage

Stage 3: Client iOS Decomposition



Mobile Client View

+ UIKit
  + NSLayout Mgr
  + NSTextAttachment
  + NS Text Container
  + UI Activity
  + UI Pasteboard

OR

Use JSON!

Model Client Controller

+ NSManaged Object
+ NSObject
  + AVCapture Input
  + AC Account Credential
  + AC AccountStore

Stage IV - Threat Enumeration for Mobile Apps

- Identify Mobile Based Threats
  - Data sources sought
  - Channel of attack (Attack Vector)
  - Threat Agents (*Actors* conducting the attacks)
- Threats based upon actual or industry related threats & prior targeted circumstances
- Validate trust boundaries defined in Stage III – Application Decomposition
- Frames up Stages V & VI
  - Targeted testing based upon identified threat patterns
  - Begin to support threat enumeration with potential abuse cases

Mobile Threat Enumeration Artifact

Application Component	Use	Possible Threat(s)
Compiled Client Executable(s) (jar)	Used to run the application	Impersonated compiled app
Other Installed Java Apps	Provides distinct uses but may be invoked by other apps depending on permissions set	Leveraging functionality of other apps in order to see if they may be leveraged in order to execute a misuse case or exploit.
Connected Limited Device Configuration (CLDC v1.1)	Java run time libraries and virtual machines (KVMs)	Exploiting vulns in libraries or overwhelming the performance of the application via saturated calls to VMs
File/ Directory Objects (manifest files)	Use to manage both configuration and app related data	Sensitive application data can be stored in these files and illicitly read by other apps or copied
Smartphone memory card	Physical auxiliary memory storage to phone RAM	Can be read by other apps anytime since persistently stored
Smartphone RAM	Temporary memory storage for apps and phone data	Shared by all phone functions and apps; no proper segregation of data
Mobile Information Device Profile (MIDP)/ Midlets	API Specification for Smartphones/ apps that leverage MIDP/ CLDC frameworks	Untrusted Midlets could intercept API calls from other platform sources

Landscape of Threats is Large

- ❑ **Denial of Service Attacks (DoS)**
  - ❑ Client & application server endpoints
- ❑ **Communication Based Threats**
  - ❑ Stealing data when its in-transit using wireless channel like 802.11, NFC based data exchange or Bluetooth based data exchange. Application Level Attacks
- ❑ **Client side attacks**
  - ❑ An adversary steals sensitive data by reading SD Card based stored content
  - ❑ An adversary exploits OS level functionalities steal data from device or server
- ❑ **Physical device theft**
  - ❑ Rooting or Jailbreaking the phone to access sensitive data from memory (physical attack vector)

- ❑ **Some threats cannot be addressed at source**
  - ❑ Carrier based threats
  - ❑ Device hardware architecture
  - ❑ Knowing these threats is nonetheless important
- ❑ **External threat intelligence**
  - ❑ Industry trends on attack vectors
  - ❑ Threat motives
  - ❑ Frames Up Stage V, VI
- ❑ **Internal threat intelligence**
  - ❑ Log/ event aggregation
  - ❑ Contextual threat intelligence
- ❑ **Prioritize Threats based upon Stage I**

External Threat Sources to Consider

- ❑ Verizon Business Annual Cybercrime report (http://www.verizonenterprise.com/DBIR/2013/)
- ❑ US CERT (http://www.us-cert.gov/mailing-lists-and-feeds)
- ❑ McAfee (http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf)
- ❑ BackOff POS Malware (https://www.us-cert.gov/ncas/alerts/TA14-212A)
- ❑ R-CISC (Retail Cyber Intelligence Sharing Center- http://www.rila.org/rcisc/Home/Pages/default.aspx) - 3 components
  - ***Retail Information Sharing & Analysis Center (ISAC****): brings retailers together for omni-directional sharing of actionable cyber threat intelligence, and functions as a conduit for retailers to receive threat information from government entities and other cyber intelligence sources.*
  - ***Education & Training****: works with retailers and partners to develop and provide both education and training to empower information security professionals in retail and related industries.*
  - ***Research****: looks to the future, undertaking research and development projects in partnership with academia, thought leaders, and subject matter experts in order to better understand threats on the horizon..'*

Stage V – Vulnerability/ Weakness Identification Mobile Security Case Study

- Seeking to find vulnerabilities, design flaws, weaknesses in codebase, system configuration, architecture
- Cover key topics around authentication, elevation of privileges, data access models as key focus
- Vulnerabilities associated with code (non-parameterized queries); Weaknesses associated with design (single application layer)
  - Mobile Code Review – static analysis will help identify vulnerable codebase and mis-configurations
  - Manual Security Testing – seeks to attempt to perform ‘fuzzing’ exercises that introduce unintended input to mobile application fields or to input parameters
  - Data Flow Diagraming can revisit security architecture model (or lack therefore for design flaws)
  - Vulnerability scanners can provide configuration gaps and software gaps on known flaws on distributed servers as part of mobile solution

What to look for: Mobile Vulns & Weakness

- **Authentication**
  - Scan/ review code that handles authentication across trust boundaries for each actors
  - Vulns/ weaknesses in Oauth models
  - Authenticity of receiver for Push Notifications/ Toasts
- **Authorization**
  - Intra-application data access permission (elevation of privileges)
  - File permissions for files created at runtime
- **Session Management**
  - Sessions do not time out; review authenticated session throughout application mode
- **Business Logic Flaws**
  - Over-scoping PHI data receive per transaction
- **Data Storage**
  - Weaknesses around sensitive data storage (retention, deletion, access, etc.)
  - Symmetric encryption keys stored on handheld
  - Weak algorithms
  - Rogue storage access allowances (e.g. - Dropbox, SIM card)
- **Web Application Vulnerabilities**
  - Injection Based Attacks (XSS & HTML Injection
  - SQL Injection
  - Command injection (shell usage – permissions)

Stage VI : Attack Modeling
Legitimizing what is ‘wrong’ in Mobile Apps

- Attack Modeling (Stage VI) focuses on exploiting identified weaknesses or vulnerabilities
  - Helps determine probability, ease of exploitation, and overall viability
  - Fuels risk analysis to consider countermeasures based upon impact, threat, identified vulnerability and probability variables
- Key Activities for this Stage
  - Build an attack tree
    - Correlate to assets (Stage II), threats (Stage IV) and Vulnerabilities (Stage V)
    - Shows logical flow of attacks in order to apply countermeasures
- Work with security testing groups in order to receive artifacts for this stage
  - Pen Test Reports

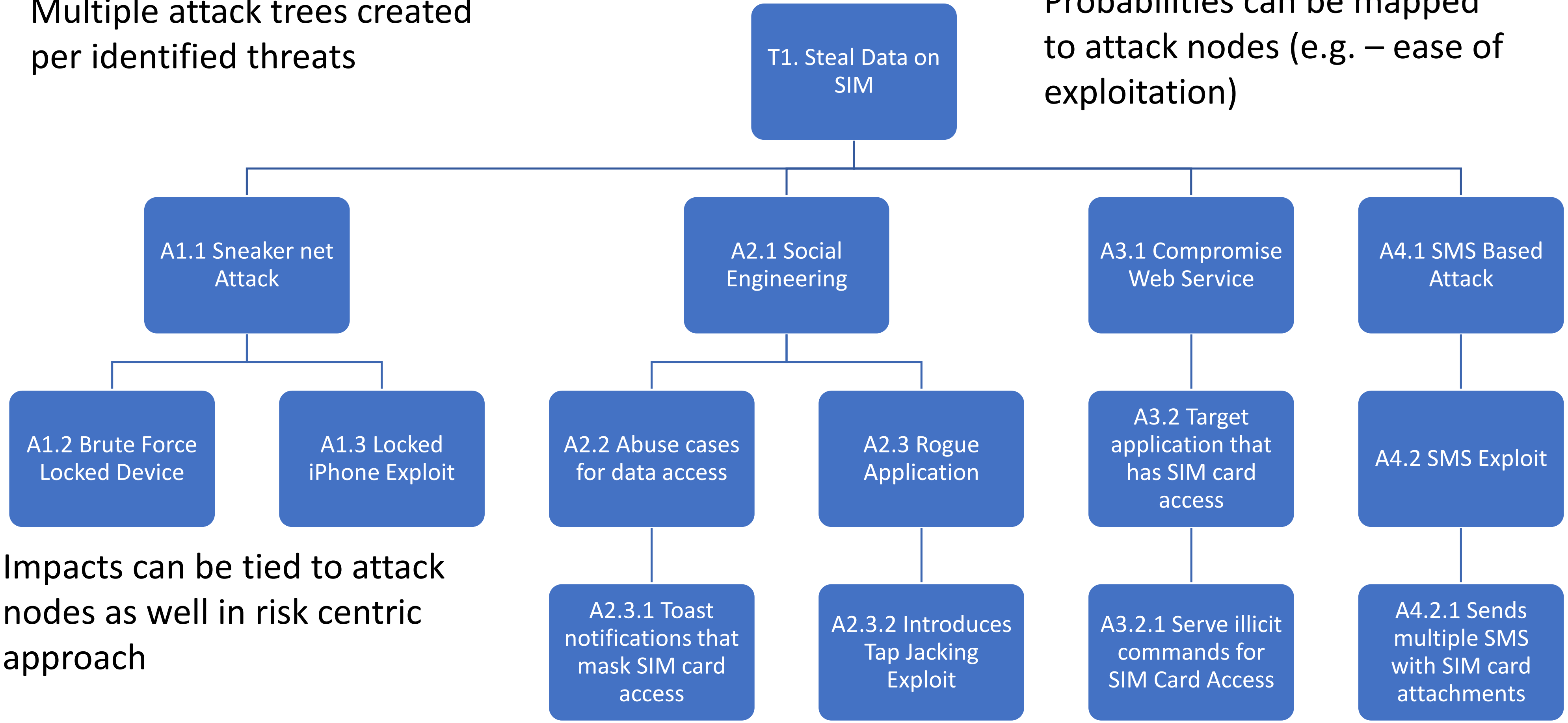
Examples of Mobile Based Attacks

- Carrier Based Methods
  - MiTM attacks using rogue wireless signal repeaters
- Endpoint based attacks
  - Many of the OWASP Top Ten Risks
    - Session fixation
    - Application fuzzing
    - Code retrieval
- Communication Based Attacks
  - Intercepting NFC, Wi-Fi communication, Bluetooth hacking
- Flash memory exploitation
- Tap jacking based attacks (mobile UI)
- Espionage/ information leakage via microphone recordings
- GPS positioning thievery

Mobile Attack Model Example

Multiple attack trees created per identified threats

Probabilities can be mapped to attack nodes (e.g. – ease of exploitation)

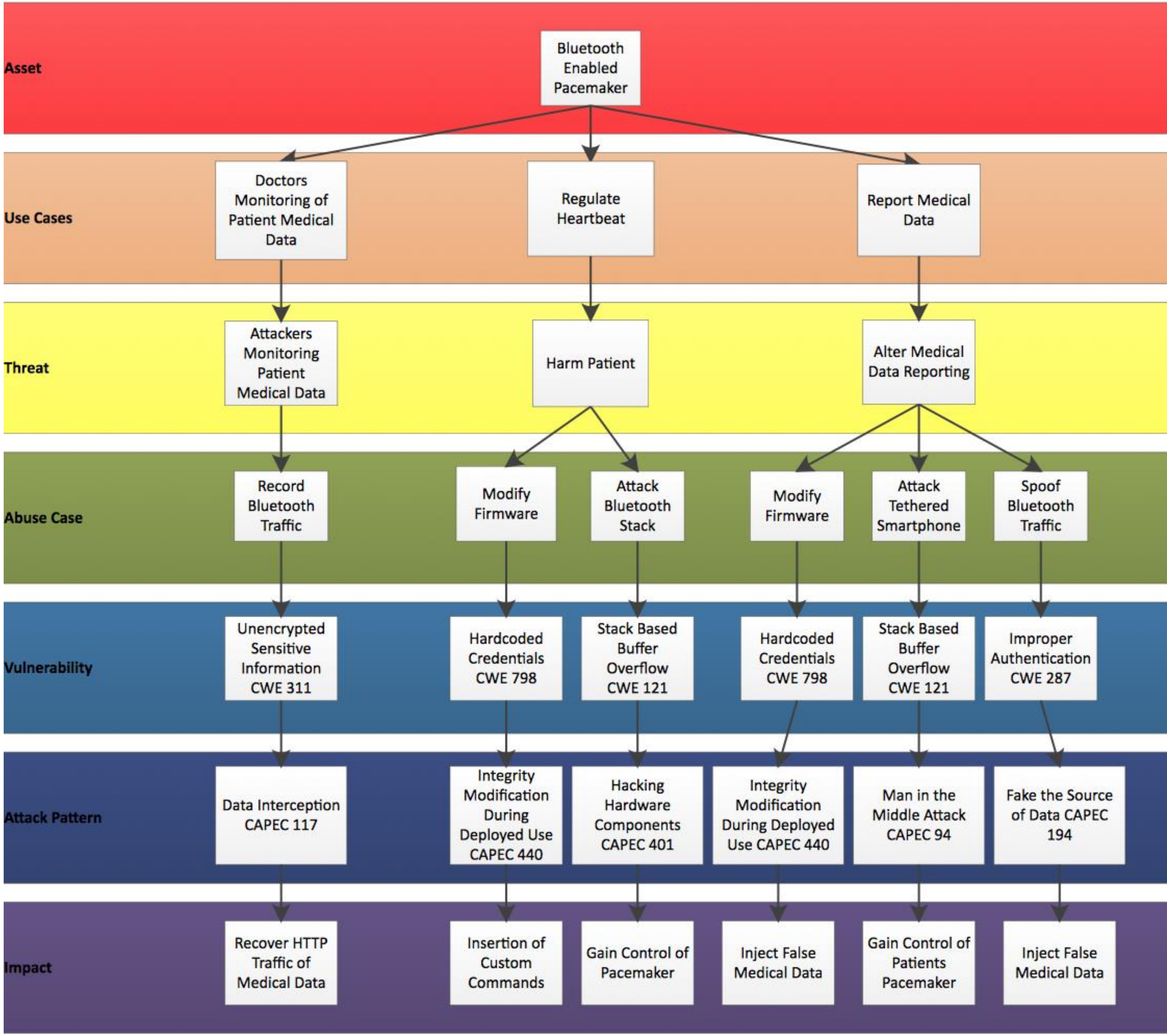


T1. Steal Data on SIM
A1.1 Sneaker net Attack
A2.1 Social Engineering
A3.1 Compromise Web Service
A4.1 SMS Based Attack
A1.2 Brute Force Locked Device
A1.3 Locked iPhone Exploit
A2.2 Abuse cases for data access
A2.3 Rogue Application
A3.2 Target application that has SIM card access
A4.2 SMS Exploit
A2.3.1 Toast notifications that mask SIM card access
A2.3.2 Introduces Tap Jacking Exploit
A3.2.1 Serve illicit commands for SIM Card Access
A4.2.1 Sends multiple SMS with SIM card attachments

Impacts can be tied to attack nodes as well in risk centric approach

Attack Tree Deliverable Sample

- Attacks support unique threats
- Threats against *People of Interest* (high value targets)
- PHI used as intel for more subtle attacks
- Bluetooth capabilities for cyber murder
- Which of the last slide’s HC threats could realize an attack node on this tree?



Asset

Bluetooth Enabled Pacemaker

Use Cases

Doctors Monitoring of Patient Medical Data

Regulate Heartbeat

Report Medical Data

Threat

Attackers Monitoring Patient Medical Data

Harm Patient

Alter Medical Data Reporting

Abuse Case

Record Bluetooth Traffic

Modify Firmware

Attack Bluetooth Stack

Modify Firmware

Attack Tethered Smartphone

Spoof Bluetooth Traffic

Vulnerability

Unencrypted Sensitive Information CWE 311

Hardcoded Credentials CWE 798

Stack Based Buffer Overflow CWE 121

Hardcoded Credentials CWE 798

Stack Based Buffer Overflow CWE 121

Improper Authentication CWE 287

Attack Pattern

Data Interception CAPEC 117

Integrity Modification During Deployed Use CAPEC 440

Hacking Hardware Components CAPEC 401

Integrity Modification During Deployed Use CAPEC 440

Man in the Middle Attack CAPEC 94

Fake the Source of Data CAPEC 194

Impact

Recover HTTP Traffic of Medical Data

Insertion of Custom Commands

Gain Control of Pacemaker

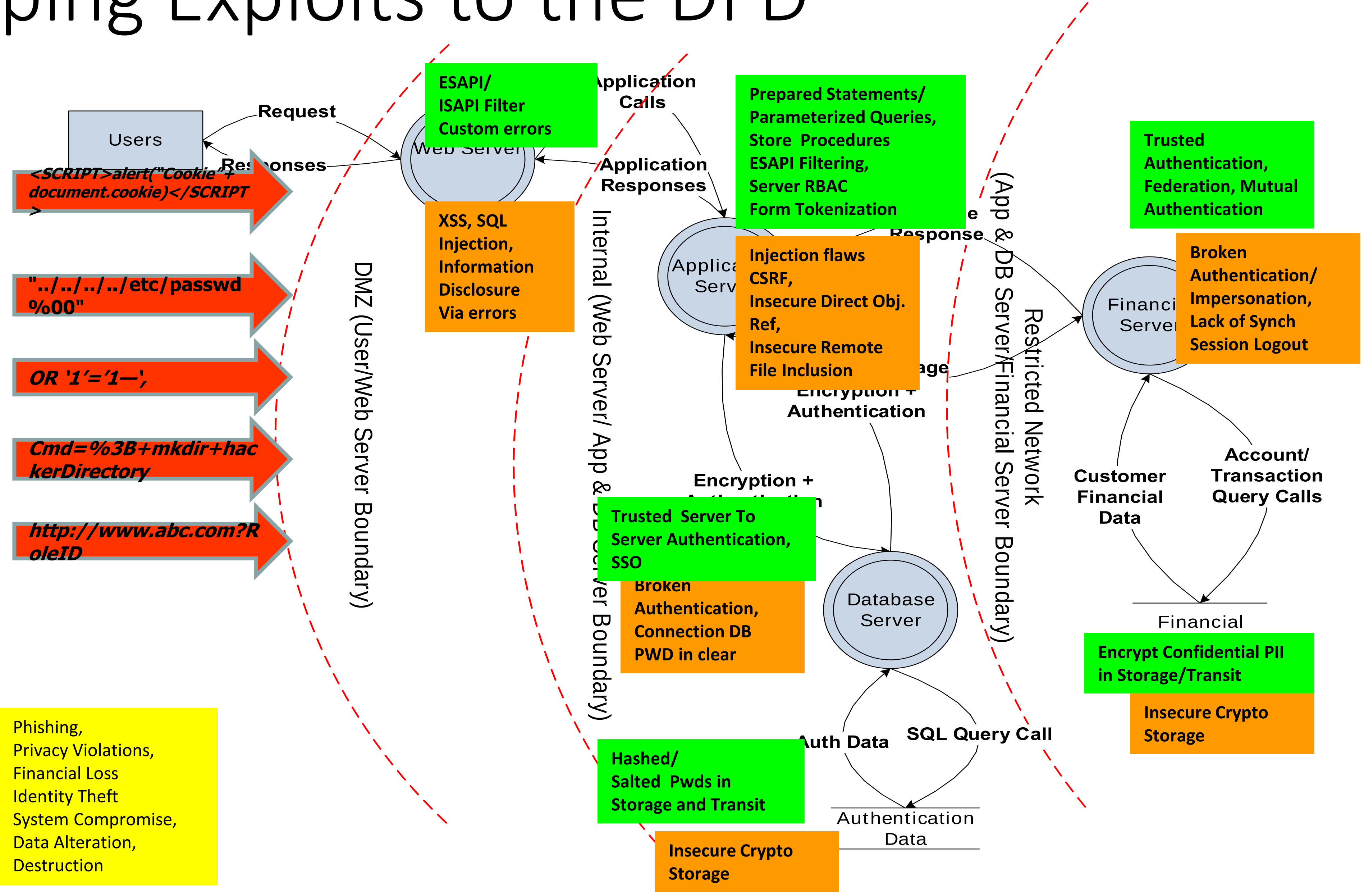
Inject False Medical Data

Gain Control of Patients Pacemaker

Inject False Medical Data

Securing What Matters in Mobile PASTA Threat modeling summary

Mapping Exploits to the DFD



Users
Request
Responses
Web Server
Application Calls
Application Responses
Applica Serv
e Response
age
Encryption + Authentication
Encryption + Authentication
Financi Server
Customer Financial Data
Account/ Transaction Query Calls
Financial
Database Server
Auth Data
SQL Query Call
Authentication Data
DMZ (User/Web Server Boundary)
Internal (Web Server/ App & DB Server Boundary)
Restricted Network (App & DB Server/Financial Server Boundary)

<SCRIPT>alert("Cookie"+ document.cookie)</SCRIPT >

"../../../../etc/passwd %00"

OR '1'='1—',

Cmd=%3B+mkdir+hackerDirectory

http://www.abc.com?RoleID

ESAPI/
ISAPI Filter
Custom errors

XSS, SQL Injection, Information Disclosure Via errors

Prepared Statements/
Parameterized Queries,
Store Procedures
ESAPI Filtering,
Server RBAC
Form Tokenization

Injection flaws
CSRF,
Insecure Direct Obj. Ref,
Insecure Remote File Inclusion

Trusted Authentication, Federation, Mutual Authentication

Broken Authentication/ Impersonation, Lack of Synch Session Logout

Trusted Server To Server Authentication, SSO

Broken Authentication, Connection DB PWD in clear

Encrypt Confidential PII in Storage/Transit

Insecure Crypto Storage

Hashed/
Salted Pwds in Storage and Transit

Insecure Crypto Storage

Phishing,
Privacy Violations,
Financial Loss
Identity Theft
System Compromise,
Data Alteration,
Destruction

Stage I & II Key Goals

- Understand business objectives for your application before criminals do
- Defines technology footprint for those involved in threat model
  - AD servers, Databases (relational/ flat file), Infrastructure, Web services (MS-WSE, WCF, REST API, JavaScript, Frameworks (OpenMEAP, etc.))
  - ARM related technology – vendor or internal?
  - Includes scope of communication protocols to be used (SSL, SSH, Bluetooth, etc.)
  - Provides scope for testing and threat analysis
- Allows opportunity for security hardening to take place
  - OEM security standards applied
  - Control frameworks leveraged (OWASP Mobile Top Ten)
  - Security primer as foundation is applied
- Tools used
  - Netstat –an (Mobile), Nmap, Dpkg, ProcessExplorer, mobile auditing software, MDM solutions
  - Application architecture schematics

Stage III Inputs/ Outputs

Stage IV Inputs

❑DFDs

❑Architectural diagrams

❑Call Flows

❑Application Manifests

❑Sniffing

Stage IV Outputs

❑Revised DFD Model

Stage IV Inputs/ Outputs

Stage IV Inputs

- ❑Threat intelligence feeds (external)
- ❑Internal alerts against mobile infrastructure (internal)
- ❑Threat synopsis
  - ▪ Short detail on inherent threats, abuse cases, threat agents taking place today on similar mobile applications.

Stage IV Outputs

- ❑Threat model diagram
  - ▪ List out top viable threats supported by research
  - ▪ Considers impact knowledge from Stage I
  - ▪ Threat Agent Enumeration
  - ▪ Abuse Case Enumeration

Stage V of PASTA Inputs/ Outputs

Stage V - Inputs

1. Technology enumeration (Stage II)
   - Provides scope of targeted vulnerability analysis
2. Threat intelligence of Mobile Application
   - Provides correlation point to which vulnerabilities/ flaws are tied to current threat scenarios
3. Business Impact
   - What do vulnerabilities mean in the context of what associated technology or vulnerable use case is supporting.

Stage V - Outputs

1. Static analysis reports
2. Vulnerability reports
3. Web application security reports (Dynamic Analysis)
4. Manual testing results
5. All of the above be aggregated, reviewed, and condensed
   - Map back to Business Objectives

Stage VI Inputs/ Outputs

Stage Inputs

1. Threat intelligence of Mobile Application
   - ❑ Provides correlation point to which vulnerabilities/ flaws are tied to current threat scenarios
2. Business Impact
   - ❑ What do vulnerabilities mean in the context of what associated technology or vulnerable use case is supporting.
3. Vulnerability Reports (Stage V)
   - ❑ Provides scope of targeted vulnerability analysis

Stage Ouputs

1. Attack Tree(s)
2. Exploitation Reports
   - ❑ What worked/ what didn’t and why?

Stage VII Inputs/ Outputs

Stage Inputs

- ❑Business Impact Analysis (Stage I)
- ❑Risk Profile (Stage 1)
- ❑Exploitation Report (Stage VI)
  - ▪ What worked/ what didn’t

Stage Outputs

- ❑Residual Risk Report Card
  - ▪ Quantifies Residual Risk
  - ▪ Remediation Roadmap
  - ▪ Precise list of recommended countermeasures

Residual Risk Analysis

- Leaders have become desensitized to risk; its meaning has warped into opinionated thought exercises
- Risk = ((Threats (probability) * Vulnerability)/Countermeasures) * Impact
- Impact assumes threat will take place
- Impact = # of occurrences * SLE
- Occurrences may equate to incidents (records lost, number of servers, etc)
- SLE = Exposure factor * Asset value

THANK YOU!

tonyuv@versprite.com

t0nyuv

VERSPRITE

www.versprite.com