CS 563 - Advanced Computer Security: Human Factors

Professor Adam Bates
Fall 2018

Administrative

Learning Objectives:

- Discuss the practical consideration of <u>usability</u> of security mechanisms and concepts
- Understand how usability can be incorporated into a broader research agenda

Announcements:

- Reaction paper was due today (and all classes)
- “Preference Proposal” Homework due 9/24

Reminder: Please put away (backlit) devices at the start of class

Why Johnny Can’t Encrypt

- Security mechanisms are only effective when used correctly
  - Invoked? configured?
- This makes security a user interface problem
- Case Study: Investigate PHP 5.0
  - Cognitive Walkthrough
  - Laboratory User Tests
- 2015 USENIX Security “Test of Time” award recipient

“Putting your text in Pig Latin isn't the same as encrypting.”

Usable Security

We can call security software/features "usable" if the people who are expected to use it…

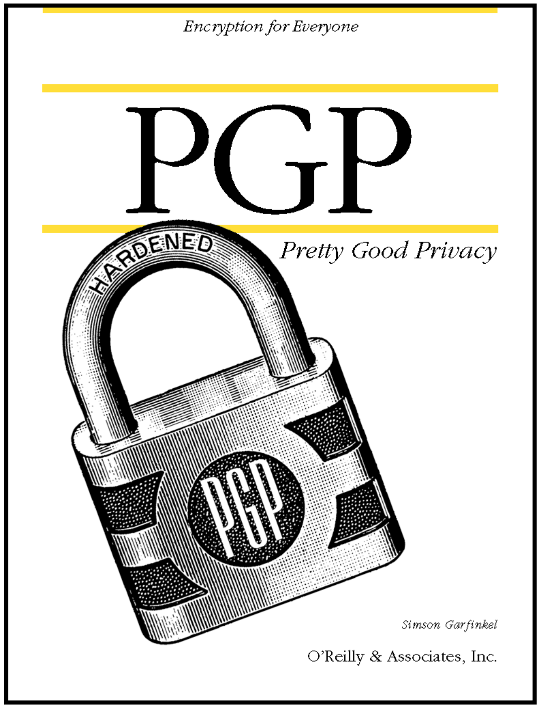
- are made aware of the tasks they need to perform
- are able to understand how to succeed at those tasks
- don't make dangerous errors while completing tasks
- are comfortable enough to continuously use the software

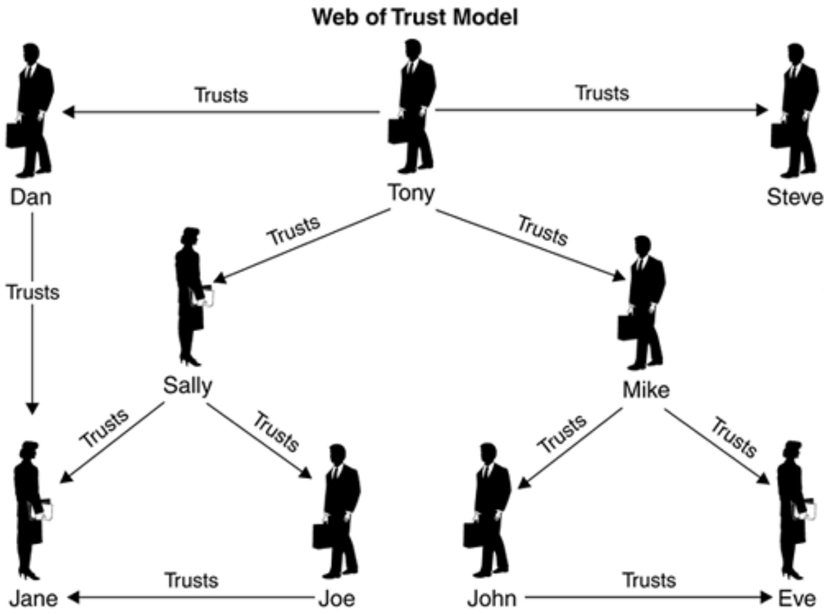
Usabile Security Challenges

- Lack of Motivation: Users will invest only limited attention/ capital to maintain security
- Understanding Abstractions: Abstractions used by domain experts (e.g., security policy) may be obtuse to end users.
- Providing good feedback: How can software guide the user to the security outcome they 'really want'?
- 'Barn Door' Property: Once an asset is unprotected even once, its security may be irrevocably compromised.
- 'Weakest Link' Property: Securing assets must be comprehensive; user engagement cannot be intermittent.

PGP 5.0

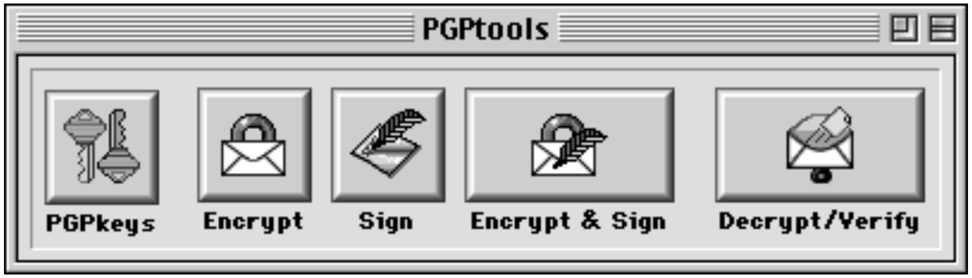
- "Pretty Good Privacy"
- Software for encrypting and signing data
- GUI with plug-in for easy (?) use with email clients

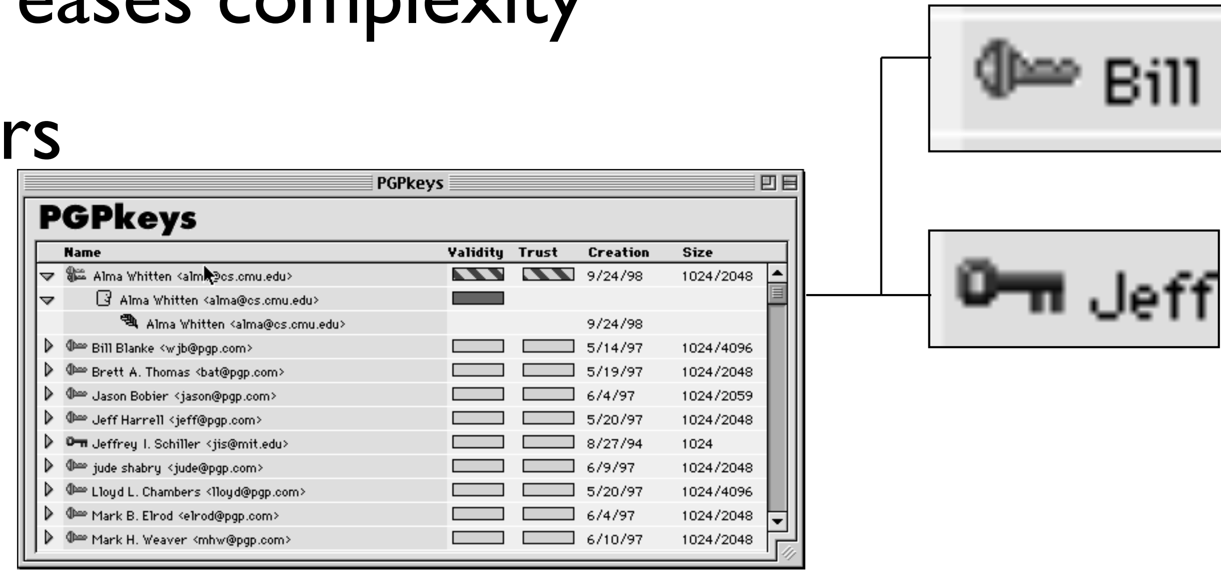




Cognitive Walkthrough

- Visual Metaphors:
  - Public vs. Private Keys
  - Signatures & Verification
- Different key types:
  - Compatibility increases complexity
  - Keys listed as users





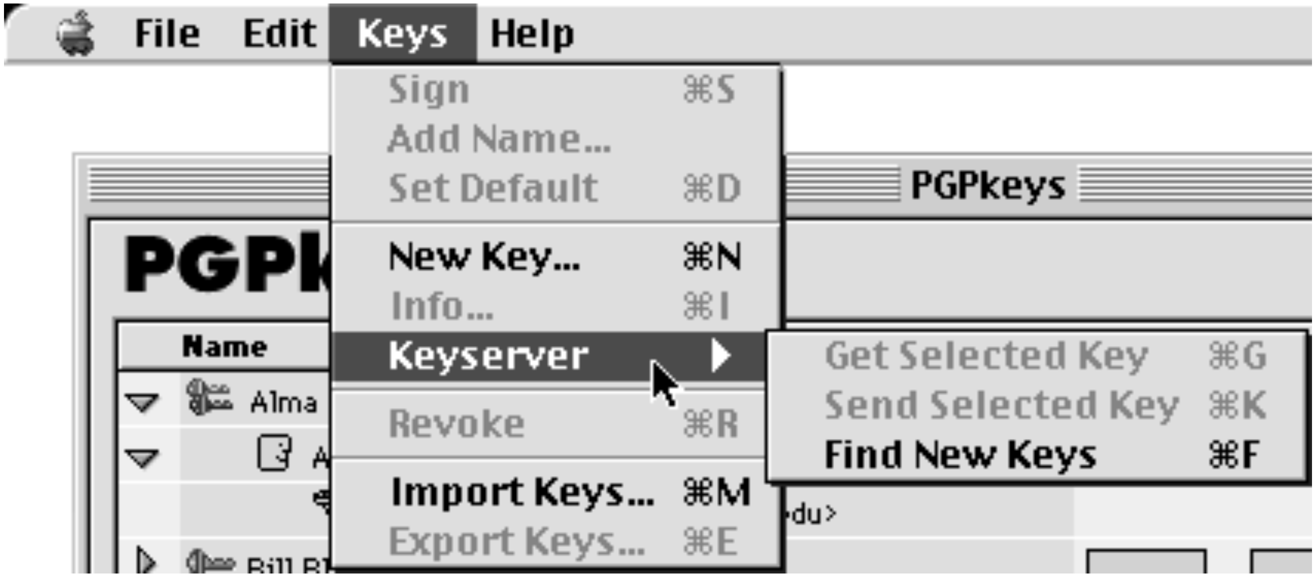
PGPkeys

PGPkeys

Name	Validity	Trust	Creation	Size
Alma Whitten <alma@cs.cmu.edu>	▨	▨	9/24/98	1024/2048
Alma Whitten <alma@cs.cmu.edu>	■			
Alma Whitten <alma@cs.cmu.edu>			9/24/98	
Bill Blanke <wjb@pgp.com>	□	□	5/14/97	1024/4096
Brett A. Thomas <bat@pgp.com>	□	□	5/19/97	1024/2048
Jason Bobier <jason@pgp.com>	□	□	6/4/97	1024/2059
Jeff Harrell <jeff@pgp.com>	□	□	5/20/97	1024/2048
Jeffrey I. Schiller <jis@mit.edu>	□	□	8/27/94	1024
jude shabry <jude@pgp.com>	□	□	6/9/97	1024/2048
Lloyd L. Chambers <lloyd@pgp.com>	□	□	5/20/97	1024/4096
Mark B. Elrod <elrod@pgp.com>	□	□	6/4/97	1024/2048
Mark H. Weaver <mhw@pgp.com>	□	□	6/10/97	1024/2048

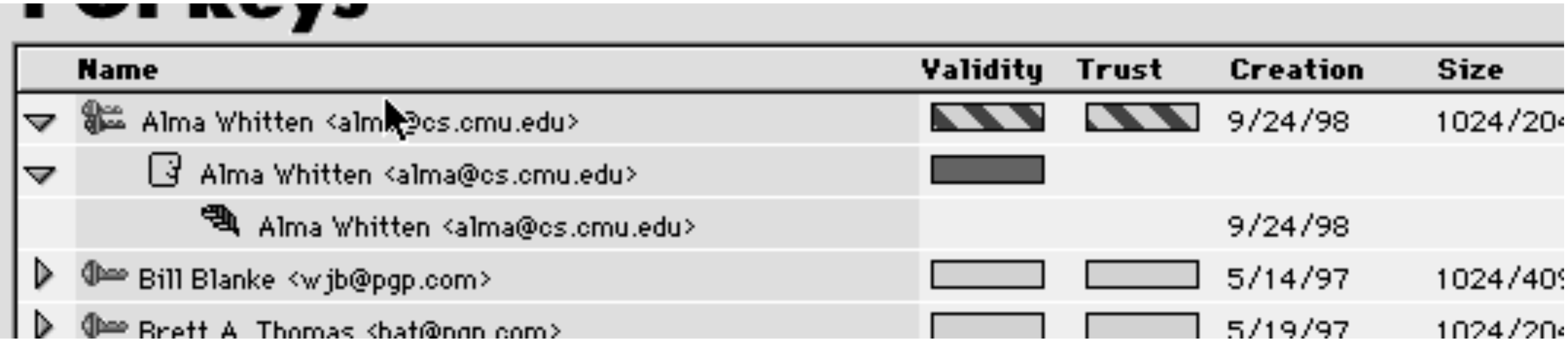
Cognitive Walkthrough

- Key Servers:
  - Vital to using PGP, but buried in menus
  - Connection to remote resource is non-obvious
  - Push for locally revoked keys is not automatic



Cognitive Walkthrough

- Key Management:
  - Unneeded confusion in interface
  - **Validity versus Trust?**



	Name	Validity	Trust	Creation	Size
▽	Alma Whitten <alma@cs.cmu.edu>	▨	▨	9/24/98	1024/20
▽	Alma Whitten <alma@cs.cmu.edu>	■			
	Alma Whitten <alma@cs.cmu.edu>			9/24/98	
▷	Bill Blanke <wjb@pgp.com>	□	□	5/14/97	1024/40
▷	Brett A. Thomas <bat@pgp.com>	□	□	5/19/97	1024/20

- Presence of Irreversible Actions (e.g., key deletion)
- Consistency of terminology
- Too much information exposed when not needed

User Tests

- PGP 5.0 with Eudora
- 12 participants all with at least some college and none with advanced knowledge of encryption
- Participants were given a scenario with tasks to complete within 90 min
- Tasks built on each other
- Participants could ask some questions through email

User Test

- Scenario: Subject is 'campaign coordinator' that needs to send private emails to campaign team.
- Tasks: Generate a key pair, acquire team's public keys, type email, sign email using private key, encrypt using team's public keys (different versions), send result.
- Experimenter posed as team member to send instructions and feedback (sidequest: decrypt message)

User Test Results

- Users sent message in plaintext (3)
- Users used their public key to encrypt (7) and could not recover (5)
- Users could not encrypt at all (1)
- Users could not decrypt messages (2 succeeded)
- Users could not handle legacy keys (1 succeeded)
- Only 3 users completed the basic process of sending and receiving encrypted emails.

Takeaway

If an average user of email feels the need for privacy and authentication, and acquires PGP with that purpose in mind, will PGP's current design allow that person to realize what needs to be done, figure out how to do it, and avoid dangerous errors, without becoming so frustrated that he or she decides to give up on using PGP after all?

Takeaway

If an average user of email feels the need for privacy and authentication, and acquires PGP with that purpose in mind, will PGP's current design allow that person to realize what needs to be done, figure out how to do it, and avoid dangerous errors, without becoming so frustrated that he or she decides to give up on using PGP after all?

Aside: Can we fix the user?

Security Design: Stop Trying to Fix the User

- “The problem isn't the users: it's that we've designed our computer systems' security so badly that we demand the user do all of these counterintuitive things.”
- Usable security does not mean "getting people to do what we want." It means creating security that works, given (or despite) what people do.
- Schneier suggests that solution is not interventions to ‘fix’ user, but the design of systems that work in spite of the user.

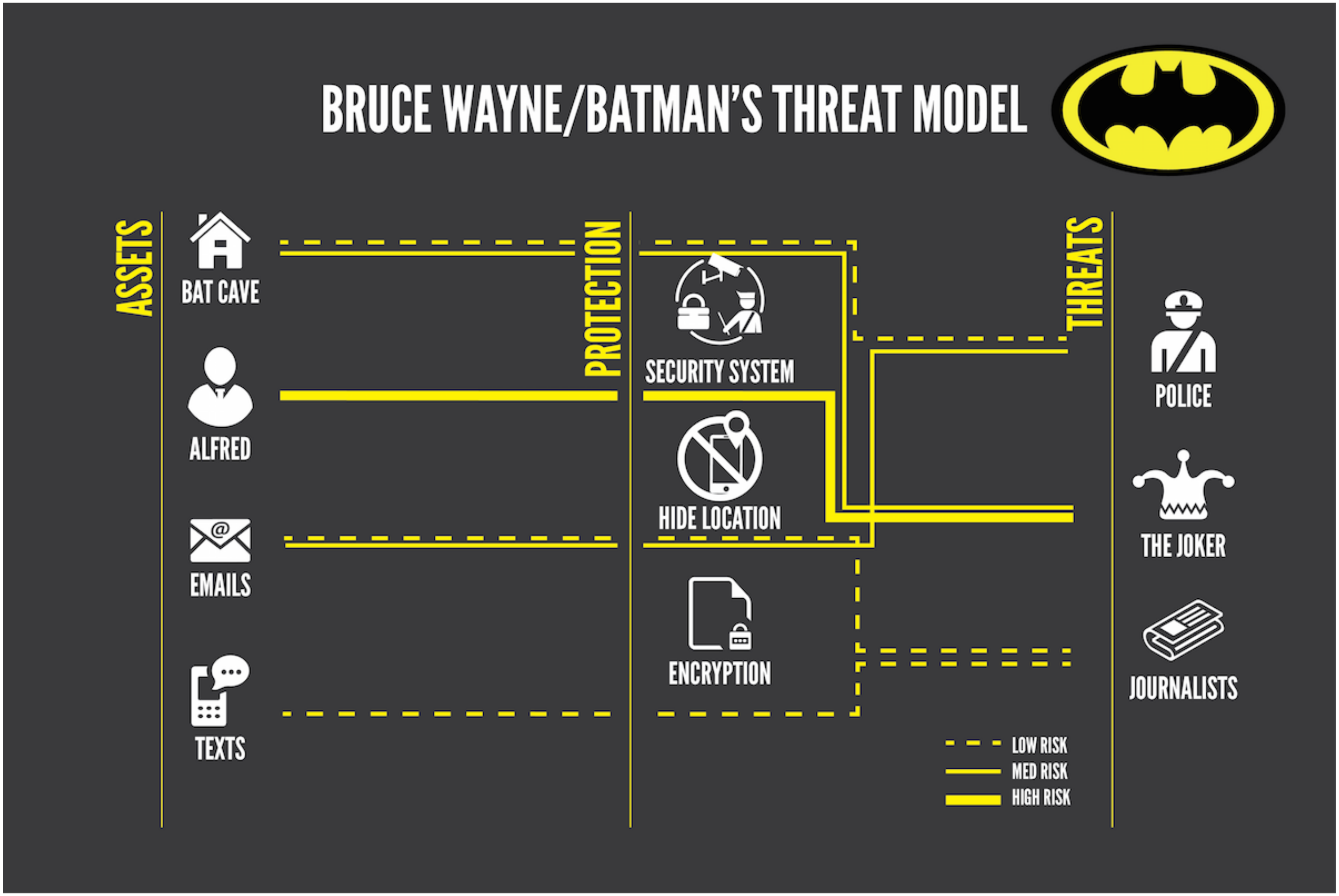
Bruce Schneier

Threat Modeling

- Foundation concept of secure system design and opsec
- *What do I want to protect?*
- *Who do I want to protect it from?*
- *How bad are the consequences if I fail?*
- *How likely is it that I will need to protect it?*
- *How much trouble am I willing to go through to try to prevent potential consequences?*

Do threat models improve real-world security?

Threat Model Example



Battle For New York

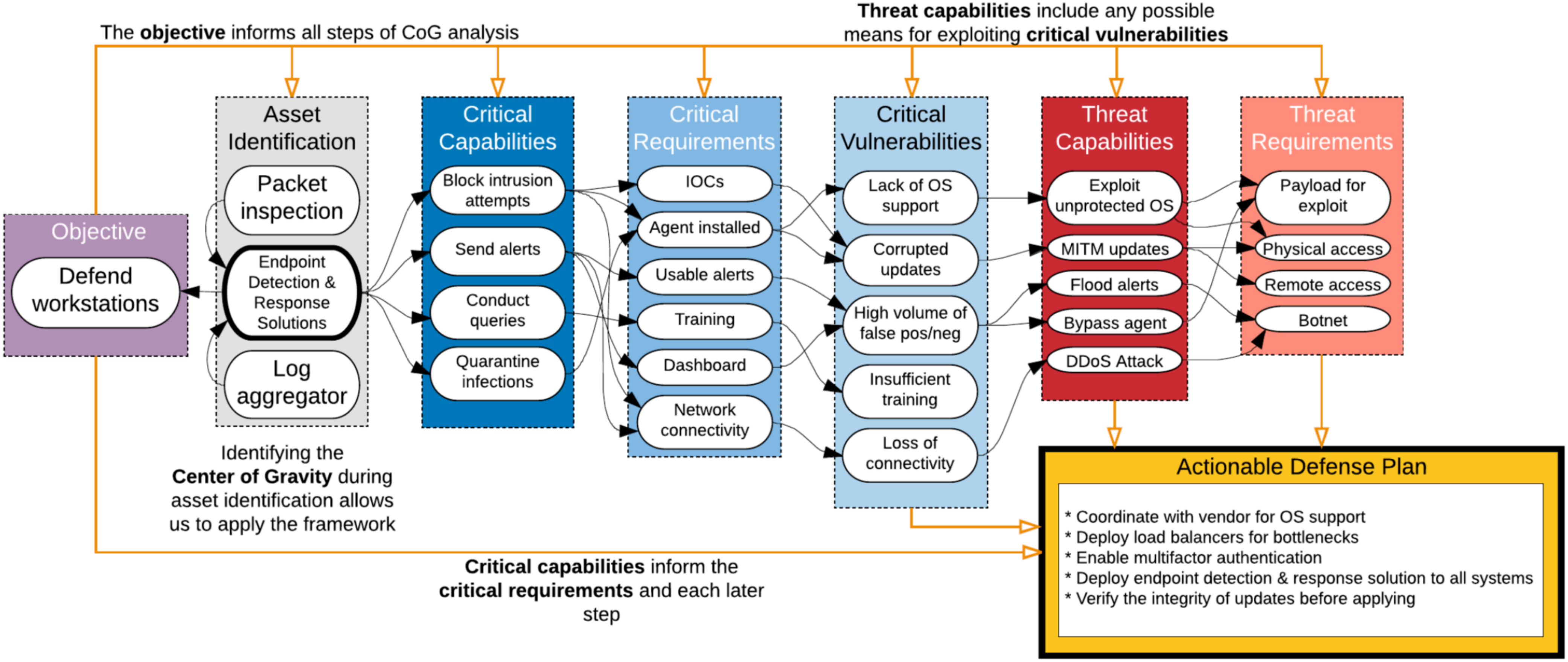
- Introduce threat modeling to New York City Cyber Command (NYC3)
- Infrastructure accessed by 60 million tourists and 300,000 employees each year
- Introduce 25 NYC3 employees to threat model training ('Center of Gravity' framework)
- Monitor their usage at 30, efficacy at 120 days

NYC®

Cyber Command

Center of Gravity Framework

- In military strategy. CoG is the primary asset(s) needed to achieve mission objective.



The **objective** informs all steps of CoG analysis

Threat capabilities include any possible means for exploiting **critical vulnerabilities**

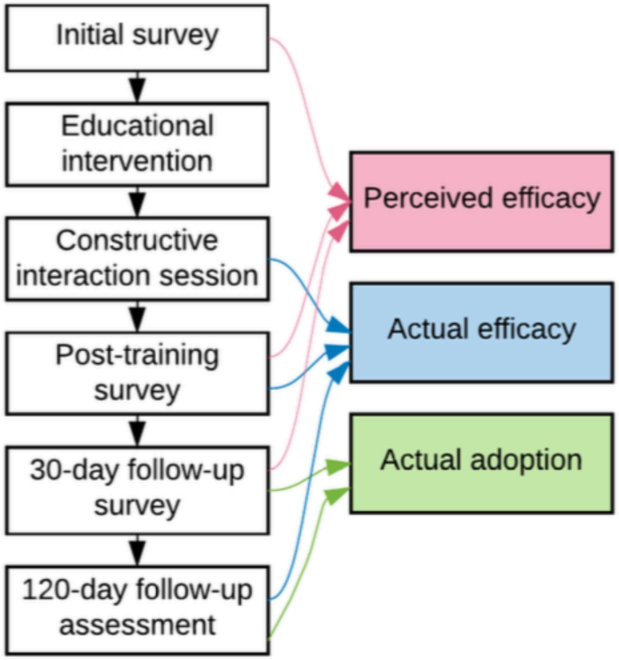
Identifying the **Center of Gravity** during asset identification allows us to apply the framework

Critical capabilities inform the **critical requirements** and each later step

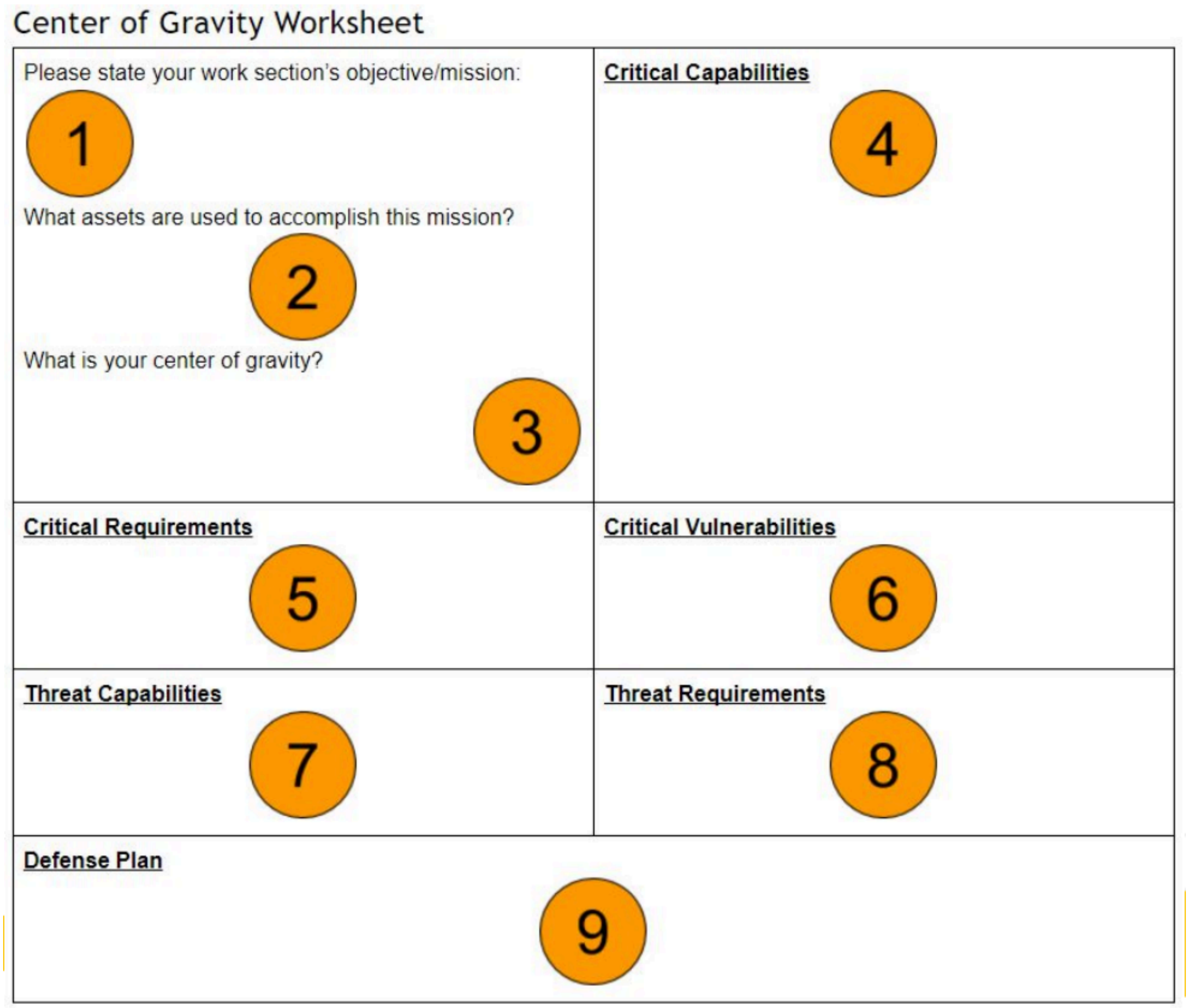
* Coordinate with vendor for OS support
* Deploy load balancers for bottlenecks
* Enable multifactor authentication
* Deploy endpoint detection & response solution to all systems
* Verify the integrity of updates before applying

Study

- Pilot study to test relevance, clarity, validity of protocol
- Recruit NYC3 employees over company email (25)
- Participants…
  - fill out 29 question baseline survey
  - complete 60 minute training
  - 60 minute individual session
  - fill out 29 question post-training survey
  - complete 30 day follow-up survey
- Long-term evaluation of security incidents at 120 days



CoG Analysis



Center of Gravity Worksheet

Please state your work section's objective/mission:

What assets are used to accomplish this mission?

What is your center of gravity?

Critical Capabilities

Critical Requirements

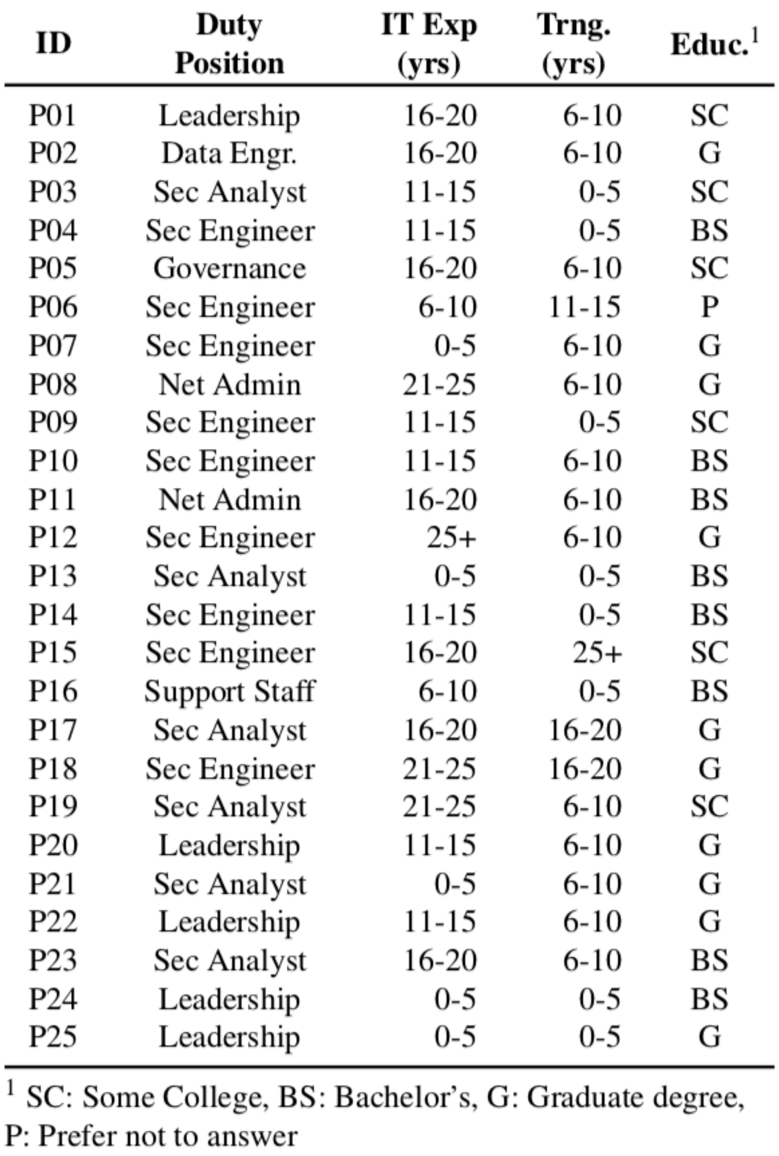
Critical Vulnerabilities

Threat Capabilities

Threat Requirements

Defense Plan

Participants



ID	Duty Position	IT Exp (yrs)	Trng. (yrs)	Educ.[1]
P01	Leadership	16-20	6-10	SC
P02	Data Engr.	16-20	6-10	G
P03	Sec Analyst	11-15	0-5	SC
P04	Sec Engineer	11-15	0-5	BS
P05	Governance	16-20	6-10	SC
P06	Sec Engineer	6-10	11-15	P
P07	Sec Engineer	0-5	6-10	G
P08	Net Admin	21-25	6-10	G
P09	Sec Engineer	11-15	0-5	SC
P10	Sec Engineer	11-15	6-10	BS
P11	Net Admin	16-20	6-10	BS
P12	Sec Engineer	25+	6-10	G
P13	Sec Analyst	0-5	0-5	BS
P14	Sec Engineer	11-15	0-5	BS
P15	Sec Engineer	16-20	25+	SC
P16	Support Staff	6-10	0-5	BS
P17	Sec Analyst	16-20	16-20	G
P18	Sec Engineer	21-25	16-20	G
P19	Sec Analyst	21-25	6-10	SC
P20	Leadership	11-15	6-10	G
P21	Sec Analyst	0-5	6-10	G
P22	Leadership	11-15	6-10	G
P23	Sec Analyst	16-20	6-10	BS
P24	Leadership	0-5	0-5	BS
P25	Leadership	0-5	0-5	G

[1] SC: Some College, BS: Bachelor's, G: Graduate degree, P: Prefer not to answer

- 25 participants completed study
- 37% of NYC3
- Pre-Intervention Baseline
  - Security assessed through city-specific policies, NIST framework, accreditation process.
  - Participants report that such guidelines were not frequently applies
  - Many were unaware of such programs

Results

- Participants reported that threat modeling gave them a better understanding of capabilities and requirements (n=12)
- Participants agreed threat modeling was useful in their daily routine (n=23)
- Many report improved ability to monitor critical assets (n=17), mitigate threats (n=16), respond to incidents (n=15)

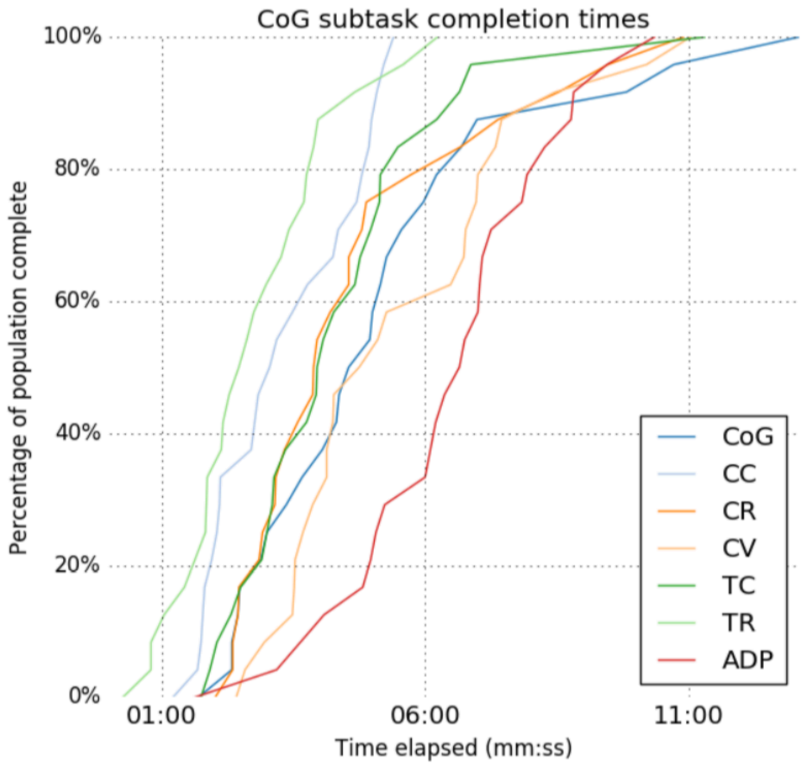


Figure 3: A cumulative distribution function (CDF) for participant subtask completion times.

Results (30 days later)

- Perceived efficacy of framework decreased only slightly (not significant)
- Still using mitigation strategies from threat modeling (n=21) or incorporating concepts into routine (n=20)
- NYC3 began to institutionalize threat modeling as a result of participant feedback

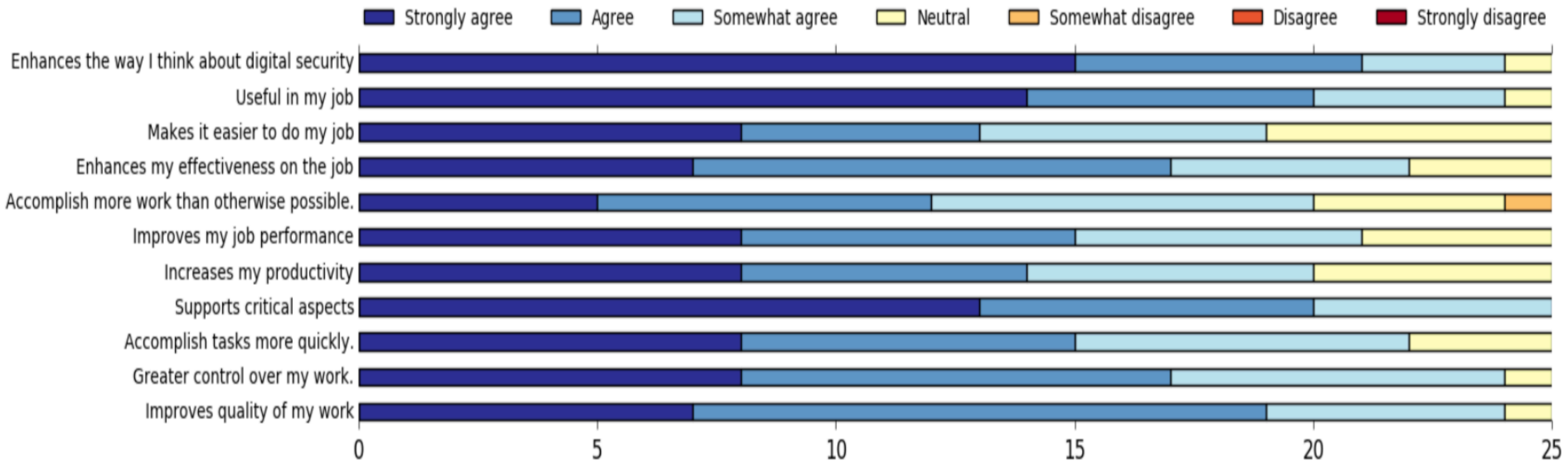


Figure 4: Perceived efficacy after using threat modeling for 30 days.

Results (120 days later)

- Inspect participants’ threat models to identify actionable defense plans:
    - Testing readiness (test defense plans)
    - Secure account permissions
    - Protect physical network assets
    - Crowdsourcing assessments (bug bounty program?)
    - Increased sensor coverage
    - Segment legacy systems
    - Protect against data corruption
    - Reduce human error (e.g., two person change control)

Results (120 days later)

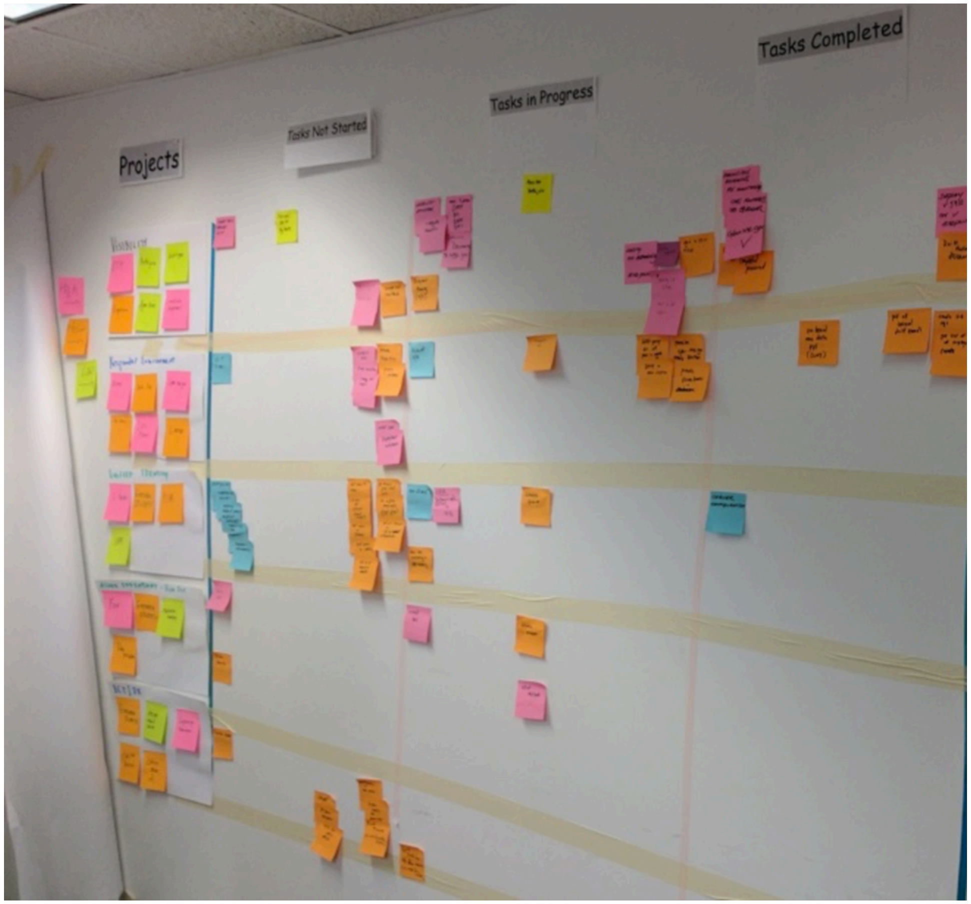
- Inspect participants' threat models to identify actionable defense plans:
  - Testing readiness (test defense plans)
  - Secure account permissions
  - Protect physical network assets
  - Crowdsourcing assessments (bug bounty program?)
  - Increased sensor coverage
  - Segment legacy systems
  - Protect against data corruption
  - Reduce human error (e.g., two person change control)

Results (120 days later)

- Inspect participants' threat models to identify actionable defense plans:
  - Secure account permissions: Seven foreign access attempts blocked because of 2FA implemented after training
  - Crowdsourcing assessments: Pilot bug bounty program yielded 3 previously-unknown vulnerabilities
  - Sensor Coverage: 1331 new endpoint sensors deployed, prevented 541 intrusion attempts (59 critical, 135 high severity).

NYC3 Takeaways

- Threat modeling facilitated adoption of ‘best practices’
- Hands-on learning is effective (n=24)
- Social and organizational support may speed adoption
- Threat modeling improved threat advocacy with leadership
- Knowledge retention (e.g., terminology) is ongoing challenge
- ***Thoughts? Limitations?***



Usable Security & You

- "Security as a secondary objective" already guides the way we design and evaluate solutions
  - ***e.g., why do we have performance evaluations?***
- Usable security methodologies allow us to measure the human capitol of systems
- If your design interacts with a human, usability <u>should</u>* be as central to your eval as any other benchmark
- Incorporating usable security into your research will give you an "unfair" advantage when publishing

Usable Security: Looking Forward

- Where to look for literature: “Big 4” security conferences (IEEE S&P a.k.a. Oakland, USENIX Security, CCS, NDSS), SOUPS workshop, security track at CHI.
- Hot Topics in Measurement (not exhaustive):
  - User Authentication (passwords, pins, meters, …)
  - Web Security, Social Networks, Secure Messaging
  - Emerging technology (IoT, VR)
  - Risk Perception, Attitude towards Privacy + Security
  - Usability of Security for Developers
  - Real World Testimony & Analysis (Enterprise, Developing World)