Pragmatic Security (in the Cloud and on Earth)

Alisson Sol, Knowledge Engineer
Engineering Excellence

May 03, 2011

Public version

Objectives

- After attending this presentation, you'll:
  - Understand why security is essential for the quality of products/services
  - Know where to go for further info about the Security Development Lifecycle (SDL)
  - Know about the trends on security attacks
  - Have a reference to model attacks based on human behavior

Takeaways and Call To Action

- Do threat models for traditional implementation bugs
- Human behavior is the weakest link exploited in most contemporary attacks on computer systems
- Do threat models for attacks based on human behavior

Evaluation of Algorithms

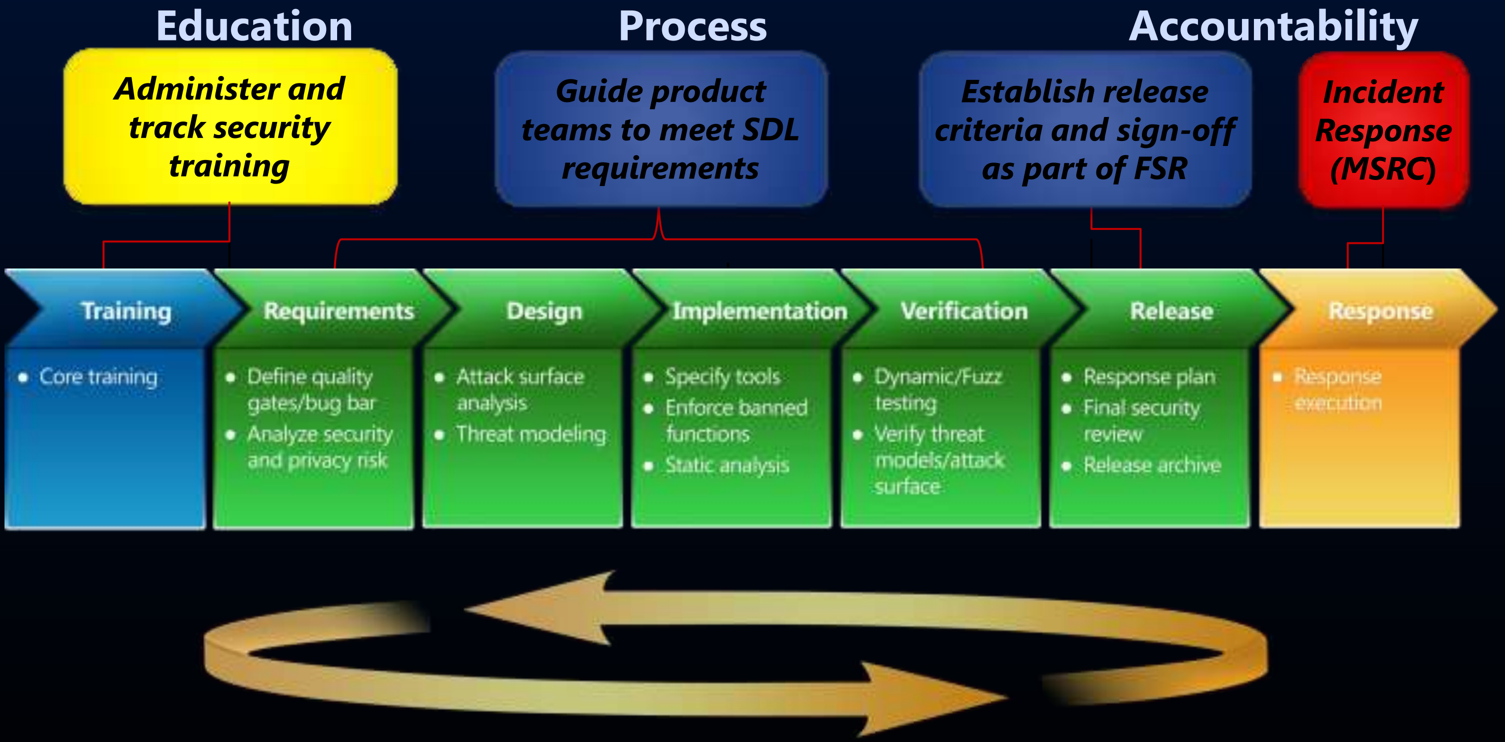
Traditional Complexity

- Memory
- Processing

Current

- Bandwidth
- Energy consumption
- Security

SDL: Security Development Lifecycle



Education

Administer and track security training

Process

Guide product teams to meet SDL requirements

Accountability

Establish release criteria and sign-off as part of FSR

Incident Response (MSRC)

Training
- Core training

Requirements
- Define quality gates/bug bar
- Analyze security and privacy risk

Design
- Attack surface analysis
- Threat modeling

Implementation
- Specify tools
- Enforce banned functions
- Static analysis

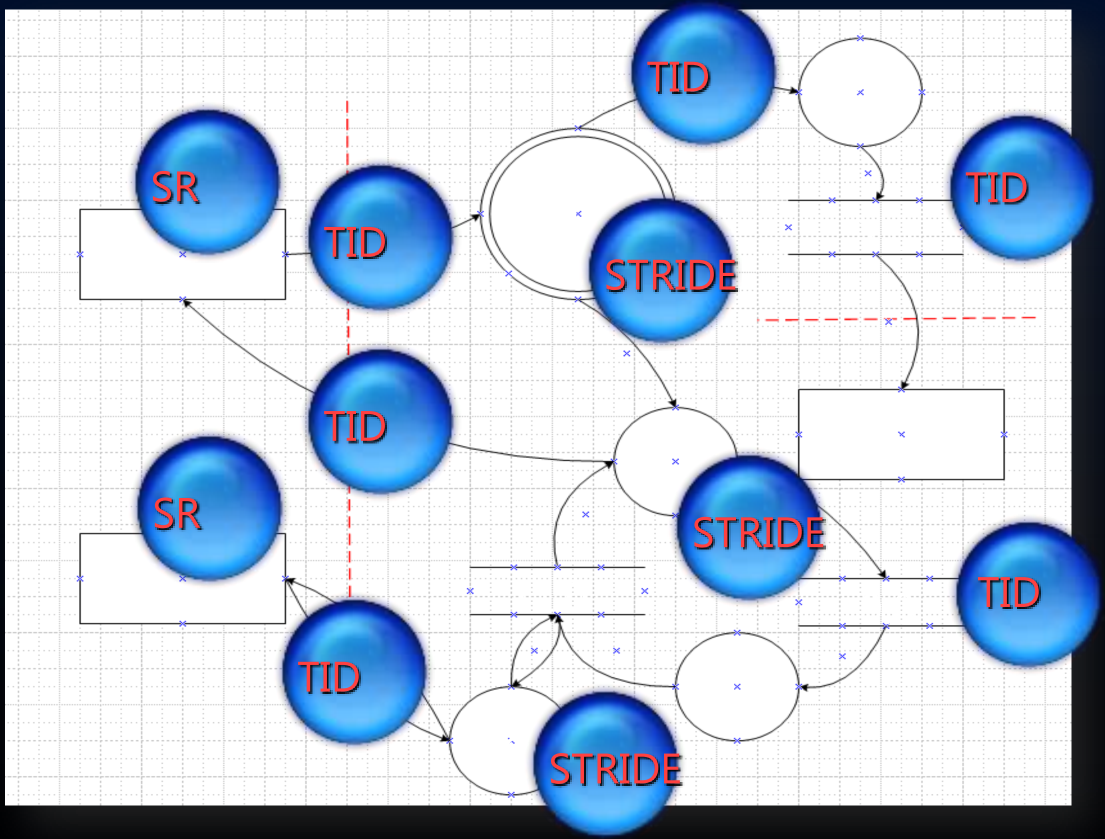
Verification
- Dynamic/Fuzz testing
- Verify threat models/attack surface

Release
- Response plan
- Final security review
- Release archive

Response
- Response execution

Ongoing Process Improvements

Threat Modeling



Each element in the Data Flow Diagram (DFD) is susceptible to one or more threat types

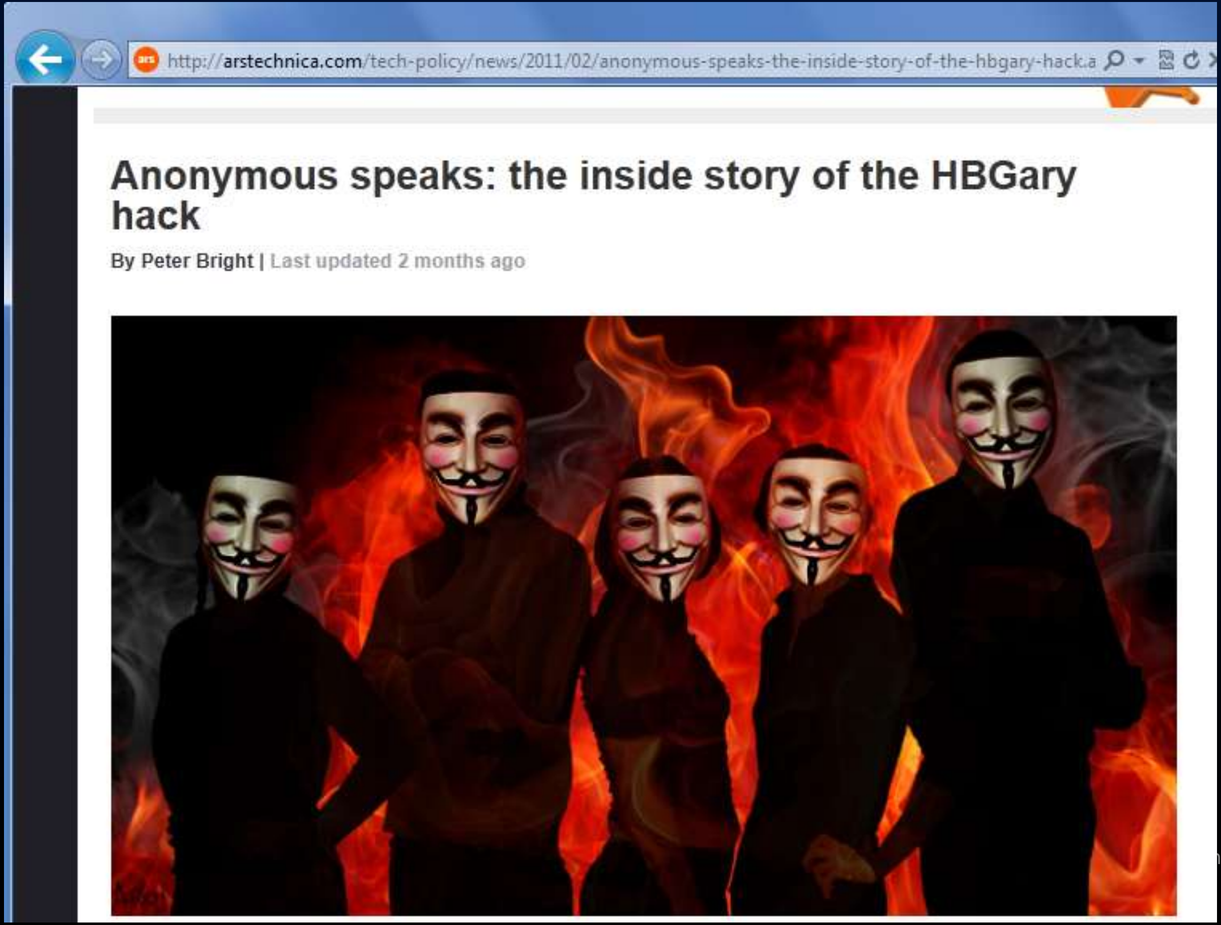
Engineering is only as good as the engineer. Be a better engineer.

Threat	Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Mitigate Everything?

- Balance: security x usability

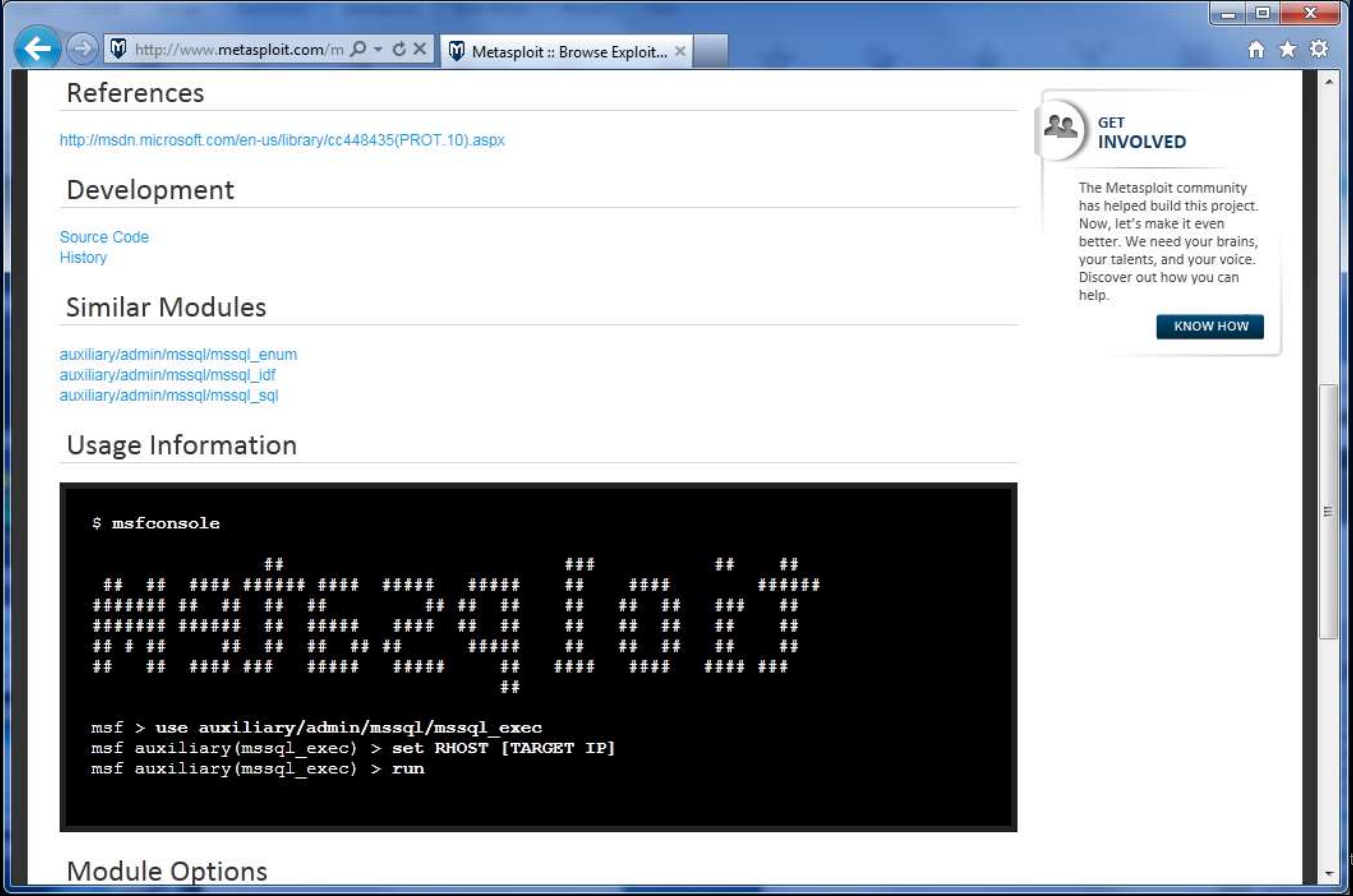
Required Knowledge For Hackers Decreasing



http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.a

Anonymous speaks: the inside story of the HBGary hack

By Peter Bright | Last updated 2 months ago



References

http://msdn.microsoft.com/en-us/library/cc448435(PROT.10).aspx

Development

Source Code
History

Similar Modules

auxiliary/admin/mssql/mssql_enum
auxiliary/admin/mssql/mssql_idf
auxiliary/admin/mssql/mssql_sql

Usage Information

```
$ msfconsole

                ##                          ###           ##    ##
 ##  ##  #### ###### ####  #####   #####    ##    ####        ######
####### ##  ##  ##  ##         ## ##  ##    ##   ##  ##   ###   ##
####### ######  ##  #####   ####  ##  ##    ##   ##  ##   ##    ##
## # ##     ##  ##  ##  ## ##      #####    ##   ##  ##   ##    ##
##   ##  #### ###   #####   #####     ##   ####   ####   #### ###
                                      ##

msf > use auxiliary/admin/mssql/mssql_exec
msf auxiliary(mssql_exec) > set RHOST [TARGET IP]
msf auxiliary(mssql_exec) > run
```

Module Options

GET
INVOLVED

The Metasploit community has helped build this project. Now, let's make it even better. We need your brains, your talents, and your voice. Discover out how you can help.

tter engineer.

http://www.microsoft.com/SDL

Microsoft Security Development Lifecycle

Write more secure software.

Watch a short video to learn how the Microsoft SDL can help your organization optimize its software security.

Highlights

The SDL Progress Report

Learn about the evolution of the SDL and the role it's played in helping Microsoft reduce vulnerabilities and develop successful threat mitigations.

MidAmerican: The SDL Chronicles

Read this compelling story about how one company improved its application security by transforming its culture and process.

Security and the Software Development Lifecycle: Secure at the Source

Read this independent Aberdeen Group research report on the positive ROI to investments in application security.

What is the Security Development Lifecycle?

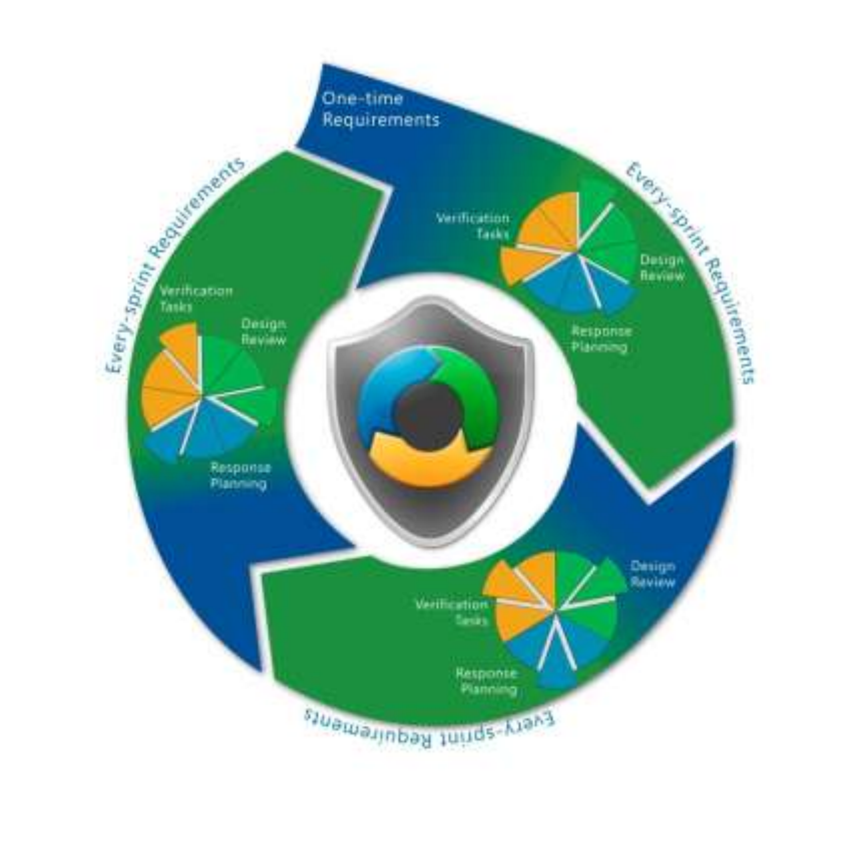
TRAINING

Assess your organizational security and privacy knowledge and establish training programs.

SDL Guidance for Agile Methodologies

- Requirements defined by frequency, not phase
  - Every-Sprint (most critical)
  - One-Time (non-repeating)
  - Bucket (all others)

- Great for projects without end dates, like cloud services

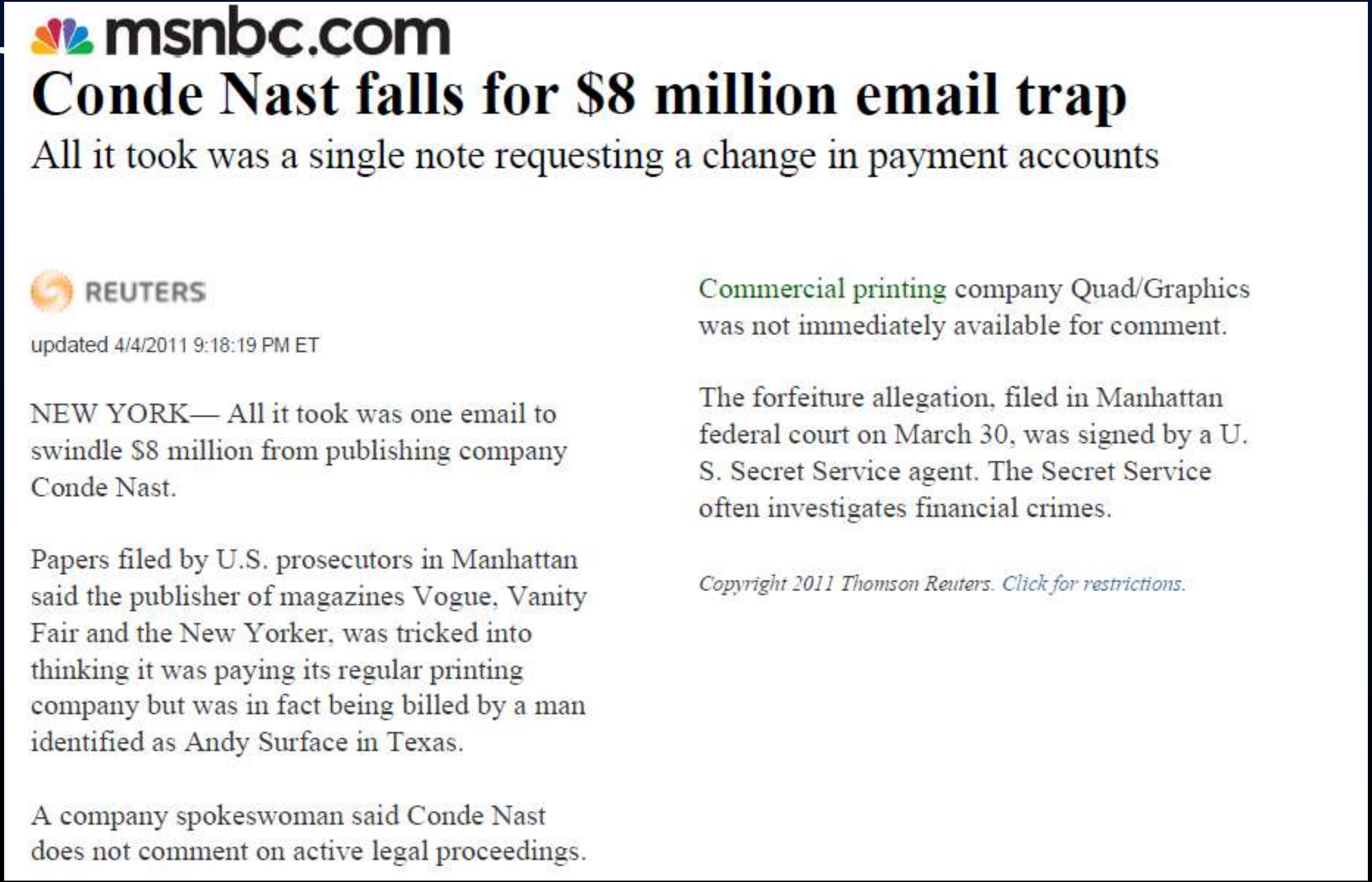


Engineering is only as good as the engineer. Be a better engineer.

Takeaways and Call To Action

- Do threat models for traditional implementation bugs
- Human behavior is the weakest link exploited in most contemporary attacks on computer systems
- Do threat models for attacks based on human behavior

Can



msnbc.com

Conde Nast falls for $8 million email trap

All it took was a single note requesting a change in payment accounts

REUTERS

updated 4/4/2011 9:18:19 PM ET

NEW YORK— All it took was one email to swindle $8 million from publishing company Conde Nast.

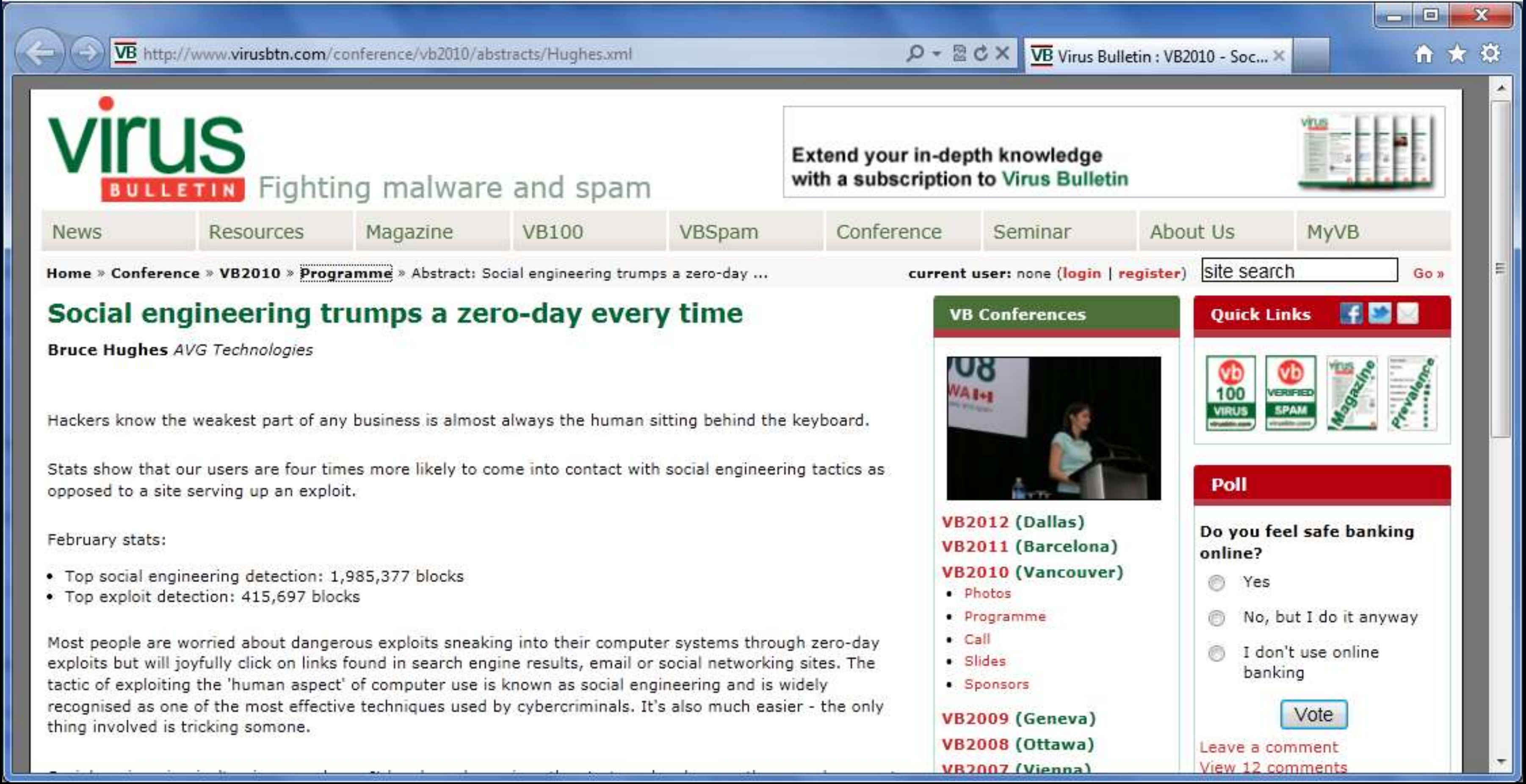
Papers filed by U.S. prosecutors in Manhattan said the publisher of magazines Vogue, Vanity Fair and the New Yorker, was tricked into thinking it was paying its regular printing company but was in fact being billed by a man identified as Andy Surface in Texas.

A company spokeswoman said Conde Nast does not comment on active legal proceedings.

Commercial printing company Quad/Graphics was not immediately available for comment.

The forfeiture allegation, filed in Manhattan federal court on March 30, was signed by a U. S. Secret Service agent. The Secret Service often investigates financial crimes.

Copyright 2011 Thomson Reuters. Click for restrictions.


http://www.virusbtn.com/conference/vb2010/abstracts/Hughes.xml
Virus Bulletin : VB2010 - Soc...
virus BULLETIN
Fighting malware and spam
Extend your in-depth knowledge with a subscription to Virus Bulletin
News
Resources
Magazine
VB100
VBSpam
Conference
Seminar
About Us
MyVB
Home » Conference » VB2010 » Programme » Abstract: Social engineering trumps a zero-day ...
current user: none (login | register)
site search
Go »

Social engineering trumps a zero-day every time

Bruce Hughes *AVG Technologies*

Hackers know the weakest part of any business is almost always the human sitting behind the keyboard.

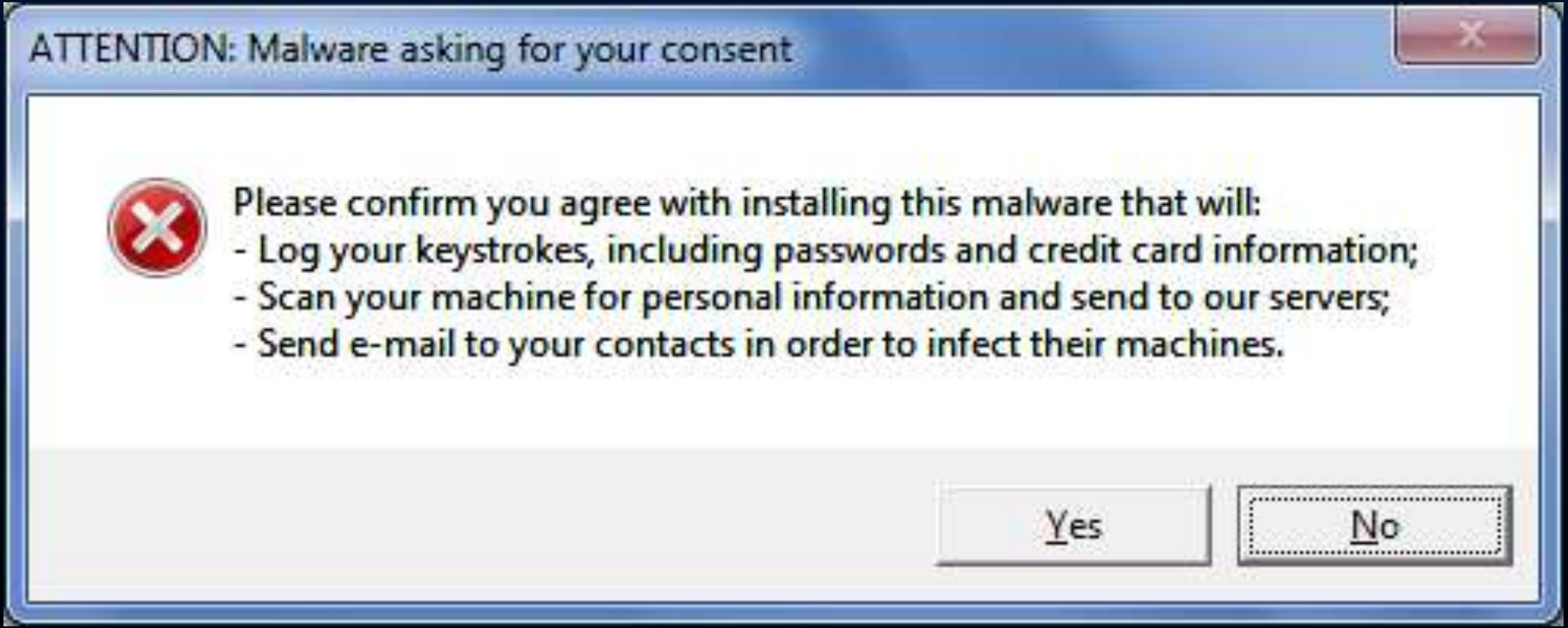
Stats show that our users are four times more likely to come into contact with social engineering tactics as opposed to a site serving up an exploit.

February stats:

- Top social engineering detection: 1,985,377 blocks
- Top exploit detection: 415,697 blocks

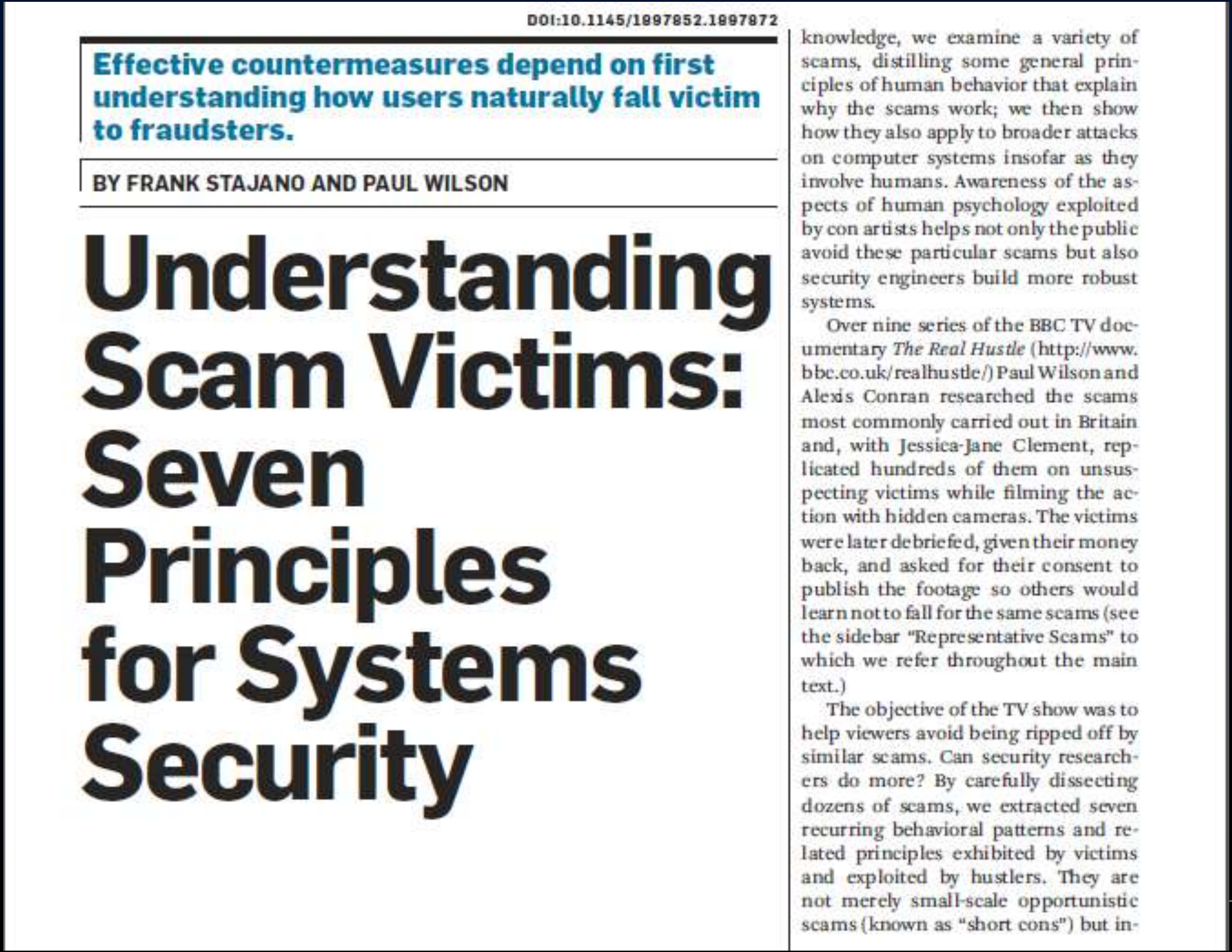
Most people are worried about dangerous exploits sneaking into their computer systems through zero-day exploits but will joyfully click on links found in search engine results, email or social networking sites. The tactic of exploiting the 'human aspect' of computer use is known as social engineering and is widely recognised as one of the most effective techniques used by cybercriminals. It's also much easier - the only thing involved is tricking somone.

Engineering is only as good as the engineer. Be a better engineer.



ATTENTION: Malware asking for your consent

Please confirm you agree with installing this malware that will:
- Log your keystrokes, including passwords and credit card information;
- Scan your machine for personal information and send to our servers;
- Send e-mail to your contacts in order to infect their machines.



DOI:10.1145/1897852.1897872

Effective countermeasures depend on first understanding how users naturally fall victim to fraudsters.

BY FRANK STAJANO AND PAUL WILSON

Understanding Scam Victims: Seven Principles for Systems Security

knowledge, we examine a variety of scams, distilling some general principles of human behavior that explain why the scams work; we then show how they also apply to broader attacks on computer systems insofar as they involve humans. Awareness of the aspects of human psychology exploited by con artists helps not only the public avoid these particular scams but also security engineers build more robust systems.

Over nine series of the BBC TV documentary *The Real Hustle* (http://www.bbc.co.uk/realhustle/) Paul Wilson and Alexis Conran researched the scams most commonly carried out in Britain and, with Jessica-Jane Clement, replicated hundreds of them on unsuspecting victims while filming the action with hidden cameras. The victims were later debriefed, given their money back, and asked for their consent to publish the footage so others would learn not to fall for the same scams (see the sidebar "Representative Scams" to which we refer throughout the main text.)

The objective of the TV show was to help viewers avoid being ripped off by similar scams. Can security researchers do more? By carefully dissecting dozens of scams, we extracted seven recurring behavioral patterns and related principles exhibited by victims and exploited by hustlers. They are not merely small-scale opportunistic scams (known as "short cons") but in-

Human Behavior Causing Vulnerabilities

- Distraction
- Social Compliance
- Herd
- Dishonesty
- Kindness
- Need and Greed
- Time

Distraction

- *While we are distracted by what grabs our interest, hustlers can do anything to us and we won't notice.*

- 2000: ILOVEYOU
  - Attachment: LOVE-LETTER-FOR-YOU.
- Nigerian scam
  - I have some millions to transfer to your account… you get 20%.

Social Compliance

- *Society trains people to not question authority. Hustlers exploit this "suspension of suspiciousness" to make us do what they want.*

- Mitnick, K.D., *The Art of Deception: Controlling the Human Element of Security*, 2002
  - Several cases of calling the police and getting information
  - Working with "someone in the chain" (receptionists, etc.)
- Message form your bank, FBI, IRS, etc.

Herd

- *Even suspicious marks let their guard down when everyone around them appears to share the same risks. Safety in numbers? Not if they're all conspiring against us.*

- Online auctions
  - Shills
  - Reputation
- Group purchases

Dishonesty

- *Our own larceny is what hooks us initially. Thereafter, anything illegal we do will be used against us by fraudsters.*

- Why most attacks go unreported?
  - *"You know you were participating in something wrong"*
- Executive laptops hacked: malware promises

Kindness

- *People are fundamentally nice and willing to help. Hustlers shamelessly take advantage of it.*

- Scams with tragic events
  - Earthquakes, tsunamis, etc.
- In most companies, people will open the door for you
  - Just show up with a packages and fake difficulties with the badge

Need and Greed

- *Our needs and desires make us vulnerable. Once hustlers know what we want, they can easily manipulate us.*
- Best way to distract people: what they crave for
  - Employment scam
- Security x usability

Time

- *When under time pressure to make an important choice, we use a different decision strategy, and hustlers steer us toward one involving less reasoning.*

- Phishing
  - Confirm your data before DD/MM/YY or you will lose access
  - Limited time discount

Are There Mitigations?

- User education
- Case-by-case model for threat and then mitigation
  - Banks log out automatically after time pass
  - Protocols requiring two people to authorize “action” (safeguard)
- Identity systems
  - Move from “*what you know*” or “*what you have*” to “*who you are*”
    - Big challenge for cloud-based systems
    - “*Please reset my password*” a top customer service request

Will Cloud Computing Change Something?

- Regarding the traditional threats
  - Increase rewards: one attack, multiple benefits
- Regarding human behavior
  - Increase attack surface: multiple opportunities for single target

Review Your Software Product/Service

- Distraction
- Social Compliance
- Herd
- Dishonesty
- Kindness
- Need and Greed
- Time

Takeaways and Call To Action

- Do threat models for traditional implementation bugs
- Human behavior is the weakest link exploited in most contemporary attacks on computer systems
- Do threat models for attacks based on human behavior

Resources

- *Understanding Scam Victims: Seven Principles for Systems Security*
  by Frank Stajano, Paul Wilson
  University of Cambridge Computer Laboratory
  Technical Report 754, August 2009
- *Understanding Scam Victims: Seven Principles for Systems Security*
  by Frank Stajano, Paul Wilson
  Communications of the ACM, Mar/2011, Vol. 54, No. 3, pp. 70-75
- *Foundations of Security: What Every Programmer Needs To Know*
  by Neil Daswani, Christoph Kern, and Anita Kesavan
- *Cloud Security and Privacy*
  by Tim Mather, Subra Kumaraswamy, Shahed Latif

Q&A

Engineering is only as good as the engineer. Be a better engineer.