(ISC)2® SECURITY CONGRESS 2012

Colocated with ASIS 2012

Defending Against Attacks by Modeling Threat Behaviors

John Benninghoff

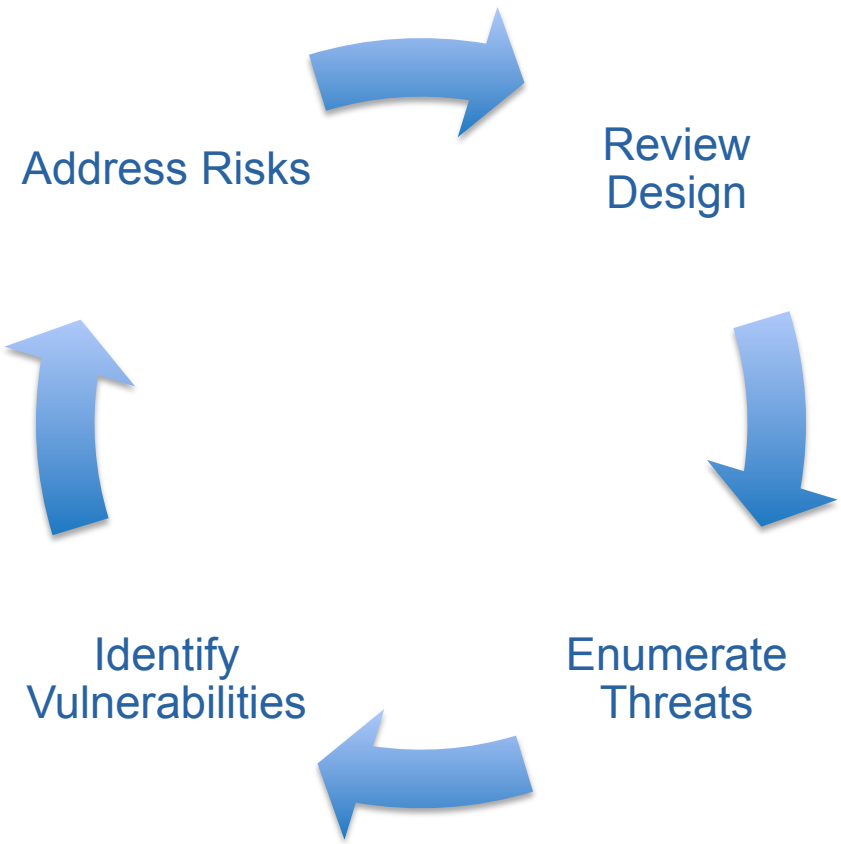
Transvasive Security

Identifying security design flaws

THREAT MODELING

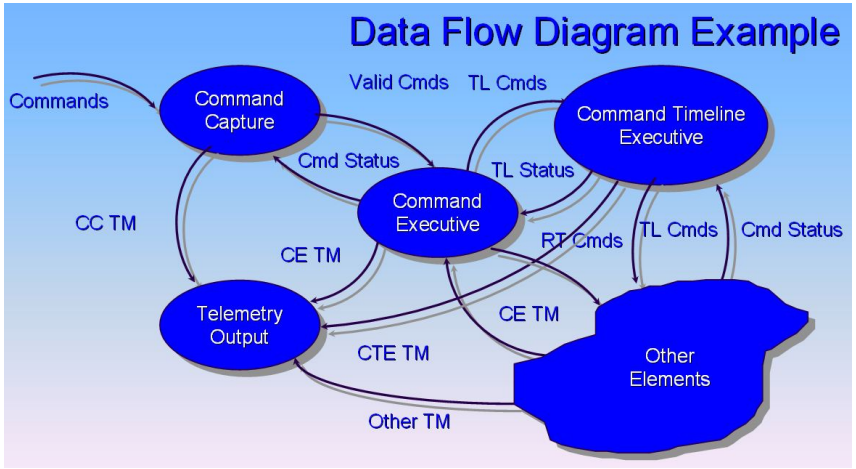
Basic Threat Modeling Approach

- Review system design
- Enumerate all possible threats
- Identify potential vulnerabilities
- Address risks



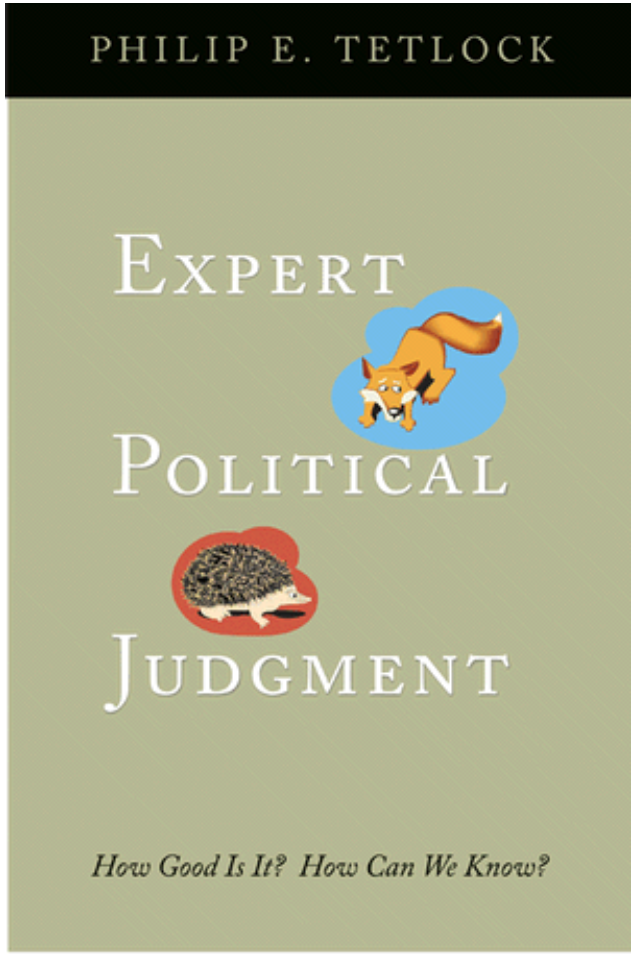
What's wrong with Threat Modeling?

- **Review system design**
- Enumerate all possible threats
- Identify potential vulnerabilities
- Address risks



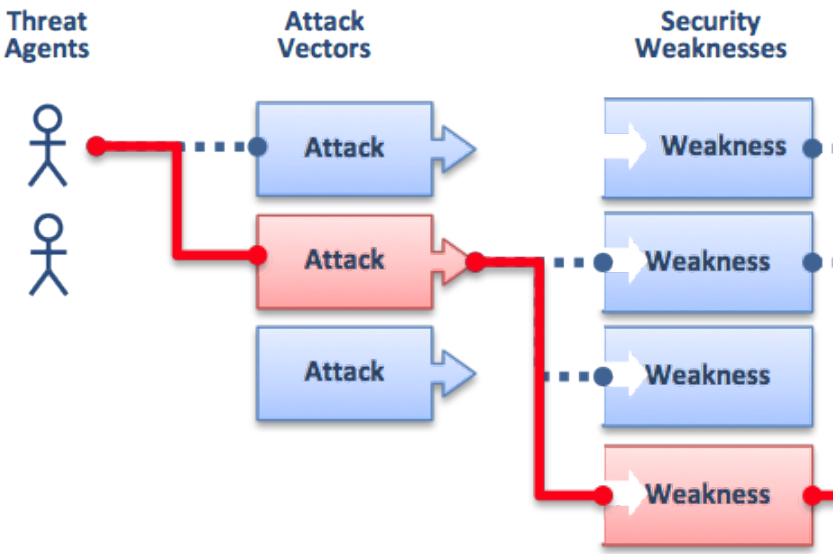
What's wrong with Threat Modeling?

- Review system design
- **Enumerate all possible threats**
- Identify potential vulnerabilities
- Address risks



What's wrong with Threat Modeling?

- Review system design
- Enumerate all possible threats
- **Identify potential vulnerabilities**
- Address risks



What's wrong with Threat Modeling?

- Review system design
- Enumerate all possible threats
- Identify vulnerabilities
- **Address risks**

Avoid

Control

Accept

Transfer

STRIDE addresses some of the problems with Threat Modeling

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Threat modeling using known threat behaviors

KNOWN UNKNOWNS

Behavioral Threat Modeling is tailored to human cognition

Behavioral Threat Modeling…

- is a way to run simulated attacks against your system in the design stage
- models actual attackers using incident and intelligence data
- is designed to be quick and easy to use
- automatically prioritizes likely threats
- is a simple model predicting “no change in current situation”

Profile attackers by their behavior, not their background

Exceptional Case Study Project

National Threat Assessment Center

Insider Threat Study (NTAC/CERT)

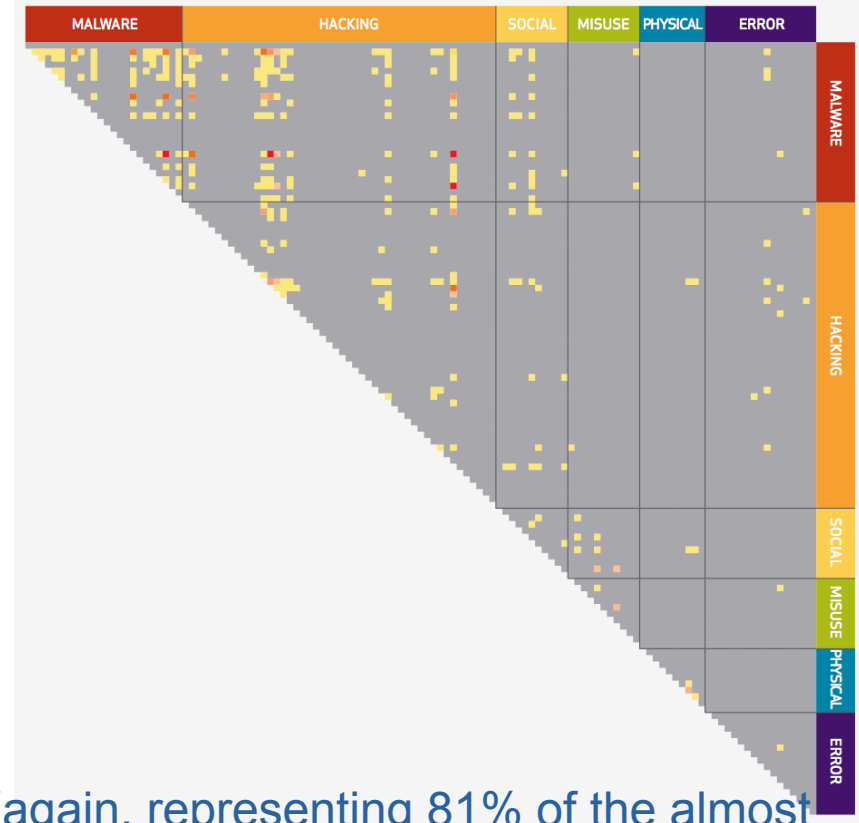
Attackers have consistent behavior patterns

2012 Verizon DBIR Threat Action pairs

Table 16. Threat Actions from top 25 pairs

malware	Keylogger/Form-grabber/Spyware (capture data from user activity)
malware	Send data to external site/entity
malware	Backdoor (allows remote access/control)
malware	Disable or interfere with security controls
hacking	Exploitation of default or guessable credentials
hacking	Exploitation of backdoor or command and control channel
hacking	Brute force and dictionary attacks
hacking	Use of stolen login credentials

Figure 51. Pairs of Threat Actions

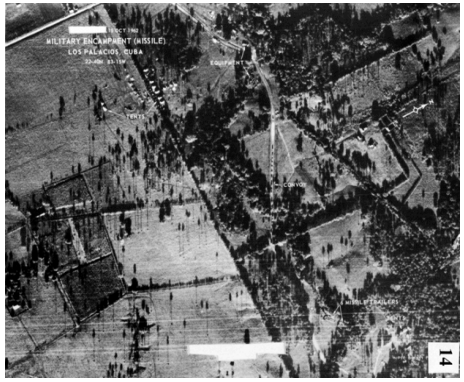


"If we look further at these top 25 pairs (again, representing 81% of the almost 4000 pairs), we see that they are just different combinations of eight threat actions …"

Attackers have consistent behavior patterns

- When malware was used to exfiltrate data, 98% of the time it was paired with keylogging functionality.
- 98% of backdoors installed were paired with exploitation of the backdoor.
- 91% of the 276 breaches leveraging stolen credentials also had keyloggers installed.
- When default or easily guessable credentials were used (in 379 incidents), 57% of the time a keylogger was installed and a backdoor was present in 47%.
- Out of the 174 backdoors installed, 61% were also seen with a keylogger.
- 73.6% of people will believe a statement that includes a statistic, even if it is completely made up.
- More analysis: http://securityblog.verizonbusiness.com

BTM uses a simple attack lifecycle



Threat Profiles describe attacks observed “in the wild”

Threat Profile: Point-of-Sale RDP Attacker

Description Attacks point-of-sale systems through RDP over the internet to install malware and exflitrate credit card numbers

Attack Phase	Agent	Action	Asset	Attribute	Frequency	Details
Preparation	External	Hacking	Offline Data	Confidentiality	Sometimes	Attacker obtains POS RDP credentials (through theft, purchase, hacking, social engineering, etc.)
Preparation	External	Hacking	Servers	Integrity	Always	Attacker compromises server systems to be used for attack, FTP servers to receive exflitrated data
Preparation	External	Hacking	Networks	Confidentiality	Always	Attacker scans internet for listening RDP servers (port 3389)
Execution	External	Hacking	Servers	Confidentiality	Always	Attacker tests a list of usernames and passwords or uses password cracking tools (guessable, stolen, brute-force)
Execution	External	Malware	Servers	Confidentiality	Always	Attacker installs malware to grab credit card numbers / magnetic stripes from credit cards used at POS system
Execution	External	Malware	Servers	Confidentiality	Always	Attacker sends credit card data to FTP site controlled by attacker
Withdrawal	External	Hacking	Servers	N/A	Always	Attacker disguises identity through use of compromised server and FTP systems

Threat Profile: Generic Malware Exfiltration

Description General pattern for malware used to steal credentials or other valuable data (credit card numbers, bank accounts, etc.)

Attack Phase	Agent	Action	Asset	Attribute	Frequency	Details
Preparation	External	Malware	User Devices	Confidentiality	Always	Attacker obtains/creates custom malware package that includes backdoors, keylogger, data exfiltration
Preparation	External	Hacking	Servers	Integrity	Always	Attacker compromises server systems to be used for attack, FTP servers to receive exflitrated data
Execution	External	Social	People	Integrity	Sometimes	Attacker runs phishing campaign (via email, social networks, etc.) to entice users to malware-infected server
Execution	External	Malware	User Devices	Confidentiality	Always	Attacker installs malware (through phishing, drive-by download, remote compromise) to grab valuable data
Execution	External	Malware	User Devices	Confidentiality	Always	Attacker sends data to FTP site controlled by attacker
Withdrawal	External	Hacking	Servers	N/A	Always	Attacker disguises identity through use of compromised server and FTP systems

Threat Profile: Generic Data Breach Discloser ("Hacktivist")

Description General pattern for attacks designed to obtain and disclose sensitive/embarassing data from specific organizations. "Hacktivist" groups sometimes follow this pattern.

Attack Phase	Agent	Action	Asset	Attribute	Frequency	Details
Preparation	External	Social	People	Integrity	Sometimes	Attacker announces campaign against target organization to recruit participants for attacks
Preparation	External	Hacking	Servers	Confidentiality	Sometimes	Attackers probe systems for vulnerabilities using vulnerability assessment tools
Preparation	External	Hacking	Servers	Integrity	Sometimes	Attackers identify open proxy servers to be used to disguise attacks
Execution	External	Hacking	Servers	Confidentiality	Always	Attackers use stolen credentials, SQL injection, dictionary and brute force attacks to gain access to sensitive data
Execution	External	Malware	Servers	Confidentiality	Always	Attacker exfiltrates stolen data
Execution	External	Malware	Servers	Confidentiality	Always	Attacker announces successful attack against target organization (when successful)
Execution	External	Hacking	Servers	Availability	Sometimes	Attacker uses recruits, hacking tools (LOIC) to execute DoS attack against target organization (when unsuccessful)
Withdrawal	External	Hacking	Servers	N/A	Sometimes	Attackers disguise identity through use of open proxy servers

Threat Profiles are built using BTM attack lifecycle and VERIS

- Attack Phase
- Attack Classification (using VERIS)
  - Agent
  - Action
  - Asset
  - Attribute
- Frequency
- Details

Threat Profile: Point-of-Sale RDP Attacker

Description Attacks point-of-sale systems through RDP over the internet to install malware

Attack Phase	Agent	Action	Asset	Attribute	Frequency
Preparation	External	Hacking	Offline Data	Confidentiality	Sometimes
Preparation	External	Hacking	Servers	Integrity	Always
Preparation	External	Hacking	Networks	Confidentiality	Always
Execution	External	Hacking	Servers	Confidentiality	Always
Execution	External	Malware	Servers	Confidentiality	Always
Execution	External	Malware	Servers	Confidentiality	Always
Withdrawal	External	Hacking	Servers	N/A	Always

Threat Profile: Generic Malware Exfiltration

Description General pattern for malware used to steal credentials or other valuable data (cr

Attack Phase	Agent	Action	Asset	Attribute	Frequency
Preparation	External	Malware	User Devices	Confidentiality	Always
Preparation	External	Hacking	Servers	Integrity	Always
Execution	External	Social	People	Integrity	Sometimes
Execution	External	Malware	User Devices	Confidentiality	Always
Execution	External	Malware	User Devices	Confidentiality	Always
Withdrawal	External	Hacking	Servers	N/A	Always

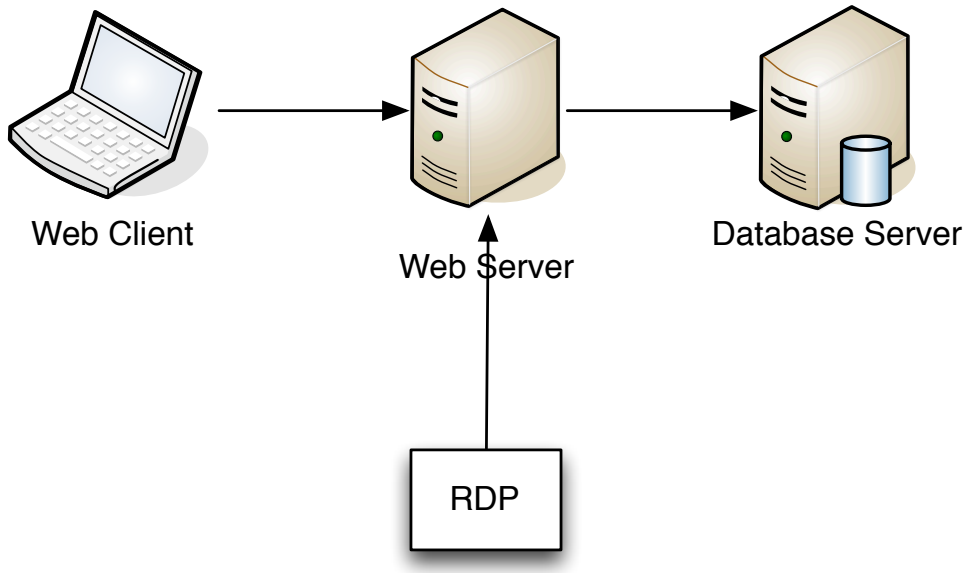
Threat Profile: Generic Data Breach Discloser ("Hacktivist")

Description General pattern for attacks designed to obtain and disclose sensitive/embarassi

Attack Phase	Agent	Action	Asset	Attribute	Frequency
Preparation	External	Social	People	Integrity	Sometimes
Preparation	External	Hacking	Servers	Confidentiality	Sometimes
Preparation	External	Hacking	Servers	Integrity	Sometimes
Execution	External	Hacking	Servers	Confidentiality	Always
Execution	External	Malware	Servers	Confidentiality	Always
Execution	External	Malware	Servers	Confidentiality	Always
Execution	External	Hacking	Servers	Availability	Sometimes
Withdrawal	External	Hacking	Servers	N/A	Sometimes

BTM system modeling is flexible

Basic Web Server Architecture



Use the threat profile and system model to simulate the attack

Threat Profile: Point-of-Sale RDP Attacker

Description Attacks point-of-sale systems through RDP over the internet to install malware

Attack Phase	Agent	Action	Asset	Attribute	Frequency
Preparation	External	Hacking	Offline Data	Confidentiality	Sometimes
Preparation	External	Hacking	Servers	Integrity	Always
Preparation	External	Hacking	Networks	Confidentiality	Always
Execution	External	Hacking	Servers	Confidentiality	Always
Execution	External	Malware	Servers	Confidentiality	Always
Execution	External	Malware	Servers	Confidentiality	Always
Withdrawal	External	Hacking	Servers	N/A	Always

Threat Profile: Generic Malware Exfiltration

Description General pattern for malware used to steal credentials or other valuable data (cr

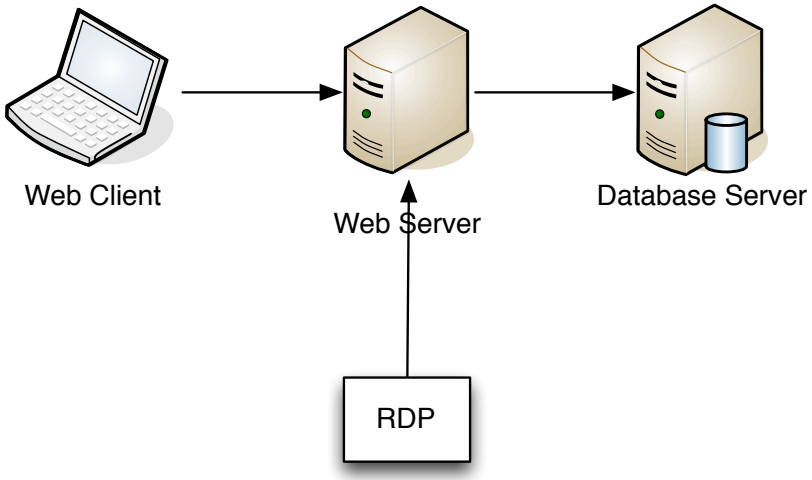
Attack Phase	Agent	Action	Asset	Attribute	Frequency
Preparation	External	Malware	User Devices	Confidentiality	Always
Preparation	External	Hacking	Servers	Integrity	Always
Execution	External	Social	People	Integrity	Sometimes
Execution	External	Malware	User Devices	Confidentiality	Always
Execution	External	Malware	User Devices	Confidentiality	Always
Withdrawal	External	Hacking	Servers	N/A	Always

Threat Profile: Generic Data Breach Discloser ("Hacktivist")

Description General pattern for attacks designed to obtain and disclose sensitive/embarassi

Attack Phase	Agent	Action	Asset	Attribute	Frequency
Preparation	External	Social	People	Integrity	Sometimes
Preparation	External	Hacking	Servers	Confidentiality	Sometimes
Preparation	External	Hacking	Servers	Integrity	Sometimes
Execution	External	Hacking	Servers	Confidentiality	Always
Execution	External	Malware	Servers	Confidentiality	Always
Execution	External	Malware	Servers	Confidentiality	Always
Execution	External	Hacking	Servers	Availability	Sometimes
Withdrawal	External	Hacking	Servers	N/A	Sometimes

Basic Web Server Architecture



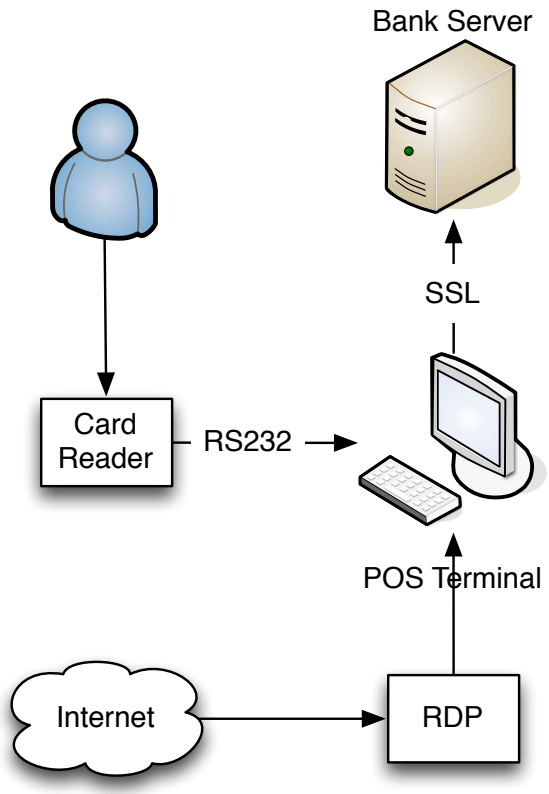
Threat Profile: POS RDP

Attack Phase	Frequency	Description
Preparation	Sometimes	Attacker obtains POS RDP credentials (through theft, purchase, hacking, social engineering, etc.)
Preparation	Always	Attacker compromises server systems to be used for attack, FTP servers to receive exflitrated data
Preparation	Always	Attacker scans internet for listening RDP servers
Execution	Always	Attacker tests a list of usernames and passwords or uses password cracking tools
Execution	Always	Attacker installs malware to grab credit card data from POS system
Execution	Always	Attacker sends credit card data to FTP site controlled by attacker
Withdrawal	Always	Attacker disguises identity through use of compromised server and FTP systems

Threat attacks POS System

Attack Sequence
Attacker obtains POS RDP credentials
Attacker compromises servers for attack
Attacker scans internet for RDP servers
Attacker uses password cracking tools
Attacker installs malware to get credit card data
Attacker sends data to FTP server
Attacker disguises identity (withdrawal)

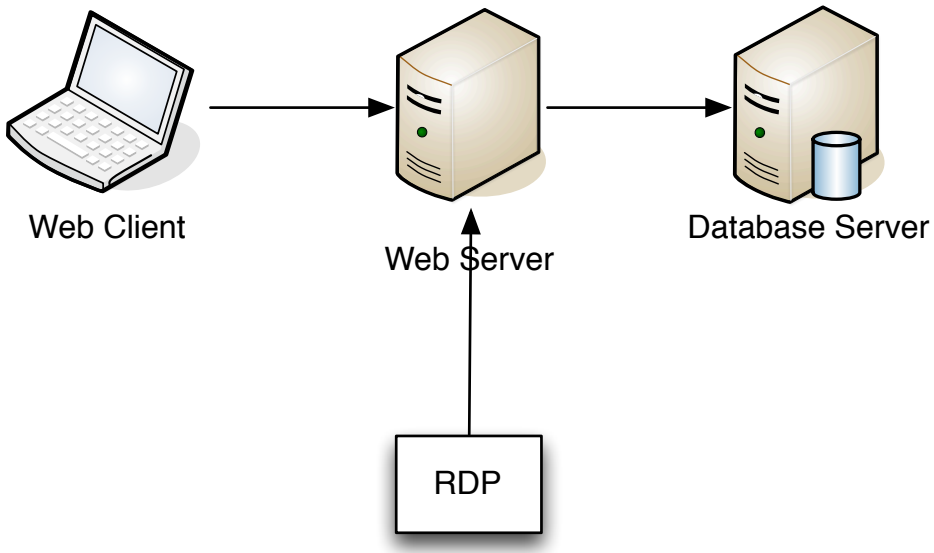
Point-of-Sale Logical Diagram



Threat attacks Web Server

Attack Sequence
Attacker obtains POS RDP credentials
Attacker compromises servers for attack
Attacker scans internet for RDP servers
Attacker uses password cracking tools
Attacker installs malware to get credit card data
Attacker sends data to FTP server
Attacker disguises identity (withdrawal)

Basic Web Server Architecture



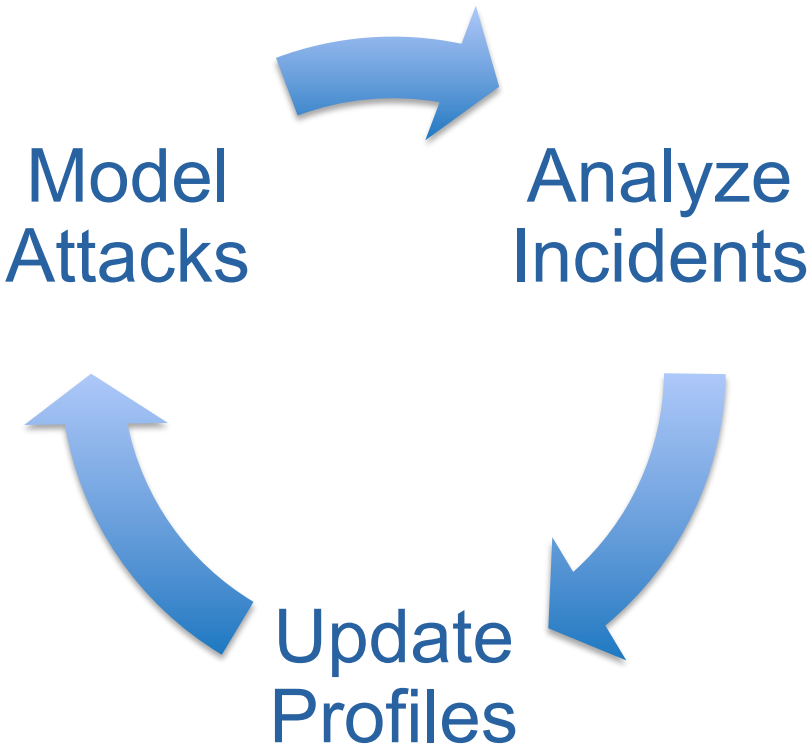
Threat Profile: Generic Malware Exfiltration

Attack Phase	Frequency	Description
Preparation	Always	Attacker obtains custom malware package that includes backdoors, keylogger, data exfiltration
Preparation	Always	Attacker compromises server systems to be used for attack, FTP servers to receive exflitrated data
Execution	Sometimes	Attacker runs phishing campaign (via email, social networks, etc.) to entice users
Execution	Always	Attacker installs malware (through phishing, drive-by, remote compromise) to grab data
Execution	Always	Attacker sends data to FTP site controlled by attacker (often using .rar)
Withdrawal	Always	Attacker disguises identity through use of compromised server and FTP systems

Threat Profile: ~~Hacktivist~~ Generic Data Breach Discloser

Attack Phase	Frequency	Description
Preparation	Sometimes	Attacker announces campaign against target organization to recruit participants for attacks
Preparation	Sometimes	Attackers probe systems for vulnerabilities using vulnerability assessment tools
Preparation	Sometimes	Attackers identify open proxy servers to be used to disguise attacks
Execution	Always	Attackers use stolen credentials, SQL injection, brute force to gain access to sensitive data
Execution	Always	Attacker exfiltrates stolen data
Execution	Always	Attacker announces successful attack against target organization (when successful)
Execution	Sometimes	Attacker uses recruits to execute DoS attack against target organization (when unsuccessful)
Withdrawal	Sometimes	Attackers disguise identity using proxy servers

Create and maintain profiles using incidents and intelligence



Elevation of Privilege card game improves STRIDE

- Created to teach developers threat modeling
- Provides several examples for each type of attack
- Ranks roughly correspond to severity of vulnerability
- Ace = “invent your own attack”

Integrate BTM into design process using three levels of review

- Level I: Self-directed “BTM on Rails” – using simple, constrained approach
- Level II: Expert-driven, “Full BTM” – using a longer list of more complex models, allow simple extrapolation
- Level III: Expert-driven, “Kitchen Sink” – discard attack chains and cycle through lists of attack behaviors

Epilogue: What can we do to prevent unknown attacks?

UNKNOWN UNKNOWNS

Safety and Emergency Response help with unknown unknowns

- Systems quality increases resistance to attack
  - Behavioral Security Modeling
  - Safety Approach
- Emergency preparedness limits damage of attacks
  - Incident response (911)
  - Disaster recovery (disaster kit)

Bonus: Behavioral Threat Modeling makes testable predictions

- BTM models predict attacks, outcomes, and can be tested through observation
- Some interesting predictions:
  - Changing default ports for internet-accessible administrative interfaces will stop attacks
  - Don’t use lowercase or numbers in your password, use uppercase and specials
  - Cross-site scripting doesn’t matter

Thank You!

Contact Information:

John Benninghoff

john@transvasive.com

http://transvasive.com/

Twitter: @transvasive

TRANSVASIVE

Transparent and Pervasive Security