Threat Models

CS 5431

February 10, 2017
Threat Models

A Crypto Nerd’s Imagination:

His laptop’s encrypted. Let’s build a million-dollar cluster to crack it.

No good! It’s 4096-bit RSA!

Blast! Our evil plan is foiled!

What Would Actually Happen:

His laptop’s encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.
Threats (CS 5430)

- Inquisitive people, unintentional blunders
- Hackers driven by technical challenges
- Disgruntled employees or customers seeking revenge
- Criminals interested in personal financial gain, stealing services, or industrial espionage
- Organized crime with the intent of hiding something or financial gain
- Organized terrorist groups attempting to influence policy by isolated attacks
- Foreign espionage agents seeking to exploit information for economic, political, or military purposes
- Tactical countermeasures intended to disrupt specific weapons or command structures
- Multifaceted tactical information warfare applied in a broad orchestrated manner to disrupt major military missions
- Large organized groups or nation states intent on overthrowing a government
## Threats (DoD)

<table>
<thead>
<tr>
<th>Tier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Practitioners who rely on others to develop the malicious code, delivery mechanisms, and execution strategy (use known exploits).</td>
</tr>
<tr>
<td>II</td>
<td>Practitioners with a greater depth of experience, with the ability to develop their own tools (from publically known vulnerabilities).</td>
</tr>
<tr>
<td>III</td>
<td>Practitioners who focus on the discovery and use of unknown malicious code, are adept at installing user and kernel mode root kits, frequently use data mining tools, target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.</td>
</tr>
<tr>
<td>IV</td>
<td>Criminal or state actors who are organized, highly technical, proficient, well funded professionals working in teams to discover new vulnerabilities and develop exploits.</td>
</tr>
<tr>
<td>V</td>
<td>State actors who create vulnerabilities through an active program to “influence” commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.</td>
</tr>
<tr>
<td>VI</td>
<td>States with the ability to successfully execute full spectrum (cyber capabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic, etc. domains and apply at scale.</td>
</tr>
</tbody>
</table>
Threats (DoD)

- **Existential**: Creates vulnerabilities using full spectrum
- **Nuisance**: Exploits pre-existing known vulnerabilities
- **Tiers I-II**: $10s
- **Tiers III-IV**: $Ms
- **Tiers V-VI**: $Bs
Threat Model = Capabilities

- privilege levels
Threat Model = Capabilities

• privilege levels
• memory access
Heartbleed
Heartbleed

How the Heartbleed Bug Works:

Server, are you still there? If so, reply "Potato" (6 letters).

User Meg wants these 6 letters: POTATO. User Lisa wants pages about "iri games". Unlocking Secure records with master key 51309057334.

Ham...

Server, are you still there? If so, reply "Hat" (500 letters).

User Meg wants these 500 letters: HAT. User Lisa requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "JohnDoeuser:1password123".
Threat Model = Capabilities

- privilege levels
- memory access
- physical access
Stuxnet
Threat Model = Capabilities

- privilege levels
- memory access
- physical access
- key access
FileVault
The iPhone Case
Humans
U.S. Election Hacks

*From:* Google <no-reply@accounts.googlemail.com>
*Date:* March 19, 2016 at 4:34:30 AM EDT
*To:* john.podesta@gmail.com
*Subject:* Someone has your password

Someone has your password
Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>

Best,
The Gmail Team
You received this mandatory email service announcement to update you about important changes to your Google product or account.
Threat Model = Capabilities

- privilege levels
- memory access
- physical access
- key access
- network access
# Network Adversaries

<table>
<thead>
<tr>
<th><strong>Attacker Properties</strong></th>
<th><strong>Membership</strong></th>
<th><strong>Method</strong></th>
<th><strong>Adaptability</strong></th>
<th><strong>Organization</strong></th>
<th><strong>Scope</strong></th>
<th><strong>Motivation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Membership</strong></td>
<td>insider</td>
<td>active</td>
<td>dynamic</td>
<td>cooperative</td>
<td>global</td>
<td>malicious</td>
</tr>
<tr>
<td><strong>Method</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>extended</td>
<td>rational</td>
</tr>
<tr>
<td><strong>Adaptability</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>opportunistic</td>
</tr>
<tr>
<td><strong>Organization</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Motivation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Pakistani YouTube Outage
Dyn DDoS
Security Goals

If someone steals my laptop while I’m logged in, they can read my email, take my money, and impersonate me to my friends, but at least they can’t install drivers without my permission.
Security Goals

- "The system shall prevent/detect *action* on/to/with *asset*."  
  - e.g., "The system shall prevent theft of money"  
  - e.g., "The system shall prevent erasure of account balances"
- Specify *what* not how
- Be specific
- Make goals *feasible* with respect to threat model